Codierungstheorie, Vorlesungsskript

Irene I. Bouw

Sommersemester 2014

Inhaltsverzeichnis

1 Lineare Codes

1.1 Einführung

Die Motivation für die Codierungstheorie kommt aus der Nachrichtenübermittlung. Wir betrachten das Problem der Übertragung von (binärer) Information über einen Kanal. Bei der Übertragung können durch Rauschen Fehler auftreten. Passiert dies, ist das empfangene Wort nicht das gleiche wie das verschickte. Um diesem Problem entgegenzuwirken, fügt man dem Informationswort extra Information hinzu. Diese extra Information kann es erlauben festzustellen, ob ein Fehler gemacht wurde und diesen möglicherweise auch zu verbessern.

Der Codierungstheorie beschäftigt sich mit dem Problem Codes zu finden, die möglichst viele Fehler korrigieren können. Ein weiteres wichtiges Problem ist es, für solche gute Codes effiziente Verfahren zu finden, die diese Fehler korrigieren.

Die Codierungstheorie ist ein relativ junger Teil der Mathematik: Sie entstand erst in den 1940er Jahren. Der erste fehlerkorrigierende Code wurde 1947 von Hamming gefunden (Abschnitt 1.5). Codes wurden beispielsweise von der NASA seit den 1970er Jahre erfolgreich bei der Übertragung von Bildern aus dem Weltall benutzt. Heutzutage ist Codierungstheorie aus dem Alltag nicht mehr wegzudenken. Codes werden beispielsweise benutzt von Handys, CD-Spielern und Cloud Computing. Bezitzt eine CD einen kleinen Kratzer, kann die gespeicherte Musik trotzdem fehlerfrei abgespielt werden. Hierbei werden Reed–Solomon-Codes benutzt (Kapitel 3).

Beispiel 1.1.1 Ein einfaches Beispiel eines Codes ist der ISBN-Code. Die am 1.1.2007 eingeführte ISBN-13-Nummer ist eine 13-stellige Zahl zur Kennzeichnung von Büchern und anderen Veröffentlichungen.

Die ISBN-13-Nummer besteht aus 4 Bestandteilen. Die Gesamtlänge für (A)–(C) ist 12 Ziffern.

(A) Die Gruppennummer (oder Ländernummer). Beispiele sind:

- 0, 1 englischsprachiger Raum (z.B. Großbritannien, USA, Australien, Indien)
- 2 französischsprachiger Raum
- 3 deutschsprachiger Raum
- 4 Japan
- 5 Russland

(B) Verlagsnummer: dies ist eine unterschiedlich lange Kennzahl für den Verlag.

(C) Titelnummer.

(D) Prüfziffer.

Vor dem 1.1.2007 wurde ein 10-stelliger ISBN-Code benutzt. Einen ISBN-10-Code kann man in einen ISBN-13-Code umwandeln, indem man vorne 978 anhängt. Die Prüfziffer muss danach neu berechnet werden.

Eine 13-stellige Zahl $x_1x_2\cdots x_{13}$ ist eine gültige ISBN-13-Nummer, falls

$$x_1 + 3x_2 + x_3 + \cdots + 3x_{12} + x_{13} \equiv 0 \pmod{10}. \tag{1.1}$$

Sind die ersten zwölf Ziffern $x_1x_2\cdots x_{12}$ gegeben, ist die Prüfziffer durch die Gleichung

$$x_{13} \equiv -(x_1 + 3x_2 + x_3 + \cdots + 3x_{12}) \pmod{10}$$

bestimmt.

Die Prüfziffer ermöglicht das Erkennen von Tippfehlern. Einer der am häufigsten gemachten Fehler beim Abtippen von ISBN-Nummern ist das Vertauschen von zwei nebeneinander gelegenen Ziffern. Dies kann man meistens mit Hilfe der Prüfziffer feststellen. Der zweithäufigste Fehler ist, dass eine Ziffer falsch eingegeben wird. Dies kann man immer feststellen.

Der ISBN-13-Code kann aber keine Fehler korrigieren. Der ISBN-13-Code

$$1\,2\,3\,4\,5\,6\,7\,8\,9\,0\,1\,2\,3$$

ist nicht gültig, da $x_1 + 3x_2 + x_3 + \cdots + 3x_{12} + x_{13} \equiv 5 \pmod{10}$. Wir können aber nicht feststellen, welche Ziffer falsch ist.

Codierung Wir wählen ein endliches Alphabet $\mathcal{A}$. Bei der Übertragung von digitalen Daten bietet sich $\mathcal{A} = \{0, 1\}$ an. *Informationswörter* $y = (y_0, y_1 \ldots, y_{k-1}) \in \mathcal{A}^k$ sind die ursprüngliche Information, die verschickt werden soll. Eine *Codierungsregel* ist eine injektive Abbildung

$$\varphi : \mathcal{A}^k \to \mathcal{A}^n, y \mapsto c$$

und bildet jedes Informationswort y auf ein *Codewort* $c = (c_0, \ldots, c_{n-1}) \in \mathcal{A}^n$ ab. Das Codewort enthält also $n-k$ zusätzliche Symbole. Beispielsweise können, wie beim ISBN-13-Code, die $n - k$ Prüfsymbole an die k Informationssymbole $y_0, \ldots, y_{k-1}$ angehängt werden.

Ein *Code* ist die Menge $\mathcal{C} := \varphi(\mathcal{A}^k) \subset \mathcal{A}^n$ der Codewörter. Die Zahl n ist die *Länge* des Codes. Die *Informationsrate* $R := k/n$ gibt an wie viele Informationssymbole ein Codewort enthält.

Beispiel 1.1.2 Wir betrachten den ISBN-Code aus Beispiel 1.1.1. Das Alphabet ist $\mathcal{A} = \{0, 1, 2, \ldots, 9\}$. Es gilt $k = 12$ und $n = 13$, also ist die Informationsrate $R = 12/13$. Die Codierungsregel ist

$$\mathcal{A}^k \to \mathcal{A}^n, \qquad (x_1, \ldots, x_{12}) \mapsto (x_1, \ldots, x_{13}),$$

wobei $x_{13} \equiv -(x_1 + 3x_2 + x_3 + \cdots + 3x_{12}) \pmod{10}$.

Senden Gegeben ist ein Codewort $c \in \mathcal{C}$. Die Codewörter werden über einen Kanal verschickt. Hierbei kann Rauschen auftreten. Sei $r = (r_0, \ldots, r_{n-1})$ das empfangene Wort und $c = (c_0, \ldots, c_{n-1})$ das gesendete Codewort. Die *Fehlerstellen* definieren wir als

$$I = \{0 \leq i \leq n-1 \mid c_i \neq r_i\}.$$

Die Kardinalität $|I|$ ist also die Anzahl der aufgetretenen Fehler. Die Hamming-Distanz wird durch die Anzahl der Fehler definiert.

Definition 1.1.3 Sei $\mathcal{A}$ ein (endliches) Alphabet und $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n) \in \mathcal{A}^n$. Die *Hamming-Distanz* ist definiert als

$$d(v, w) = |\{i \mid v_i \neq w_i\}|.$$

Ist $\mathcal{C} \subset \mathcal{A}^n$ ein Code, dann heißt

$$d_{\min}(\mathcal{C}) = \min_{v,w \in \mathcal{C}, v \neq w} d(v, w)$$

die *Minimaldistanz* von $\mathcal{C}$.

Ist $\mathcal{A} = \mathbb{F}_2 = \{0, 1\}$, dann ist die Hamming-Distanz genau das Quadrat der üblichen euklidischen Distanz. Das folgende Lemma zeigt, dass die Hamming-Distanz die üblichen Eigenschaften einer Metrik erfüllt.

Lemma 1.1.4 *Die Hamming-Distanz erfüllt*

(a) $d(v, w) = d(w, v)$,

(b) *(Dreiecksungleichung)* $d(u, w) \leq d(u, v) + d(v, w)$,

(c) $d(v, w) \geq 0$. *Die Hamming-Distanz* $d(v, w)$ *ist genau dann Null, wenn* $v = w$.

Beweis: Übungsaufgabe. □

Decodierung Der Empfänger hat das Wort r empfangen und möchte das Informationswort rekonstruieren. Dies passiert üblicherweise in zwei Schritten. Zuerst wird das Codewort c berechnet. Dann wird aus dem Codewort das Informationswort ermittelt. In diesem Skript beschäftigen wir uns hauptsächlich mit dem ersten Teil der Aufgabe.

Bevor wir uns in den weiteren Kapiteln mit konkreten Codes und Decodierverfahren beschäftigen, fragen wir uns zunächst wie viele Fehler wir korrigieren können. Wir betrachten hier die *Maximum Likelihood Decodierung*. Hierbei wird dem Wort ein Codewort c zugeordnet für das $d(r, c)$ minimal ist. Wurden sehr viele Fehler gemacht, ist das Wort c im Allgemeinen nicht mehr eindeutig. In dieser Situation wäre die Decodierung nicht eindeutig.

Das folgende Lemma gibt eine Aussage über die Anzahl der Fehler, die wir maximal korrigieren können.

Definition 1.1.5 Ein Code, der alle Fehlermuster vom Gewicht $\leq t$ korrigieren kann, heißt *t-fehlerkorrigierend*. Die *Fehlerkorrekturrate* ist definiert als t/n.

Lemma 1.1.6 *Sei $\mathcal{C} \subset \mathcal{A}^n$ ein Code mit Minimaldistanz d. Der Code $\mathcal{C}$ ist genau dann t-fehlerkorrigierend, wenn $t \leq \lfloor (d-1)/2 \rfloor$ ist.*

Die Bedingung $t \leq \lfloor (d-1)/2 \rfloor$ ist äquivalent zu $t < d/2$.

Beweis: Sei $\mathcal{C}$ ein Code mit Minimaldistanz d und sei $t = \lfloor (d-1)/2 \rfloor$. Wir nehmen an, dass $\mathcal{C}$ nicht t-fehlerkorrigierend ist. Dann existieren ein Wort r und zwei Codewörter c_1, c_2 mit $d(r, c_i) \leq t$. Lemma 1.1.4 impliziert, dass $d(c_1, c_2) \leq d(r, c_1) + d(r, c_2) \leq 2t < d$. Die Definition der Minimaldistanz impliziert, dass $c_1 = c_2$.

Ist umgekehrt $\mathcal{C}$ ein t-fehlerkorrigierender Code, dann unterscheiden sich zwei verschiedene Codewörter $c_1, c_2 \in \mathcal{C}$ an mindestens $2t+1$-Stellen. Also ist die Minimaldistanz mindestens $2t+1$. □

Beispiel 1.1.7 Die Minimaldistanz des ISBN-Codes ist $d = 2$. Beispielsweise sind 9783037190012 und 8793037190012 beide gültige ISBN-Nummern.

Lemma 1.1.6 impliziert also, dass wir keine Fehler korrigieren können. Dies hatten wir in Beispiel 1.1.1 schon gesehen.

Beispiel 1.1.8 Der Wiederholungscode mit Parameter $k = 1$ und $n = 2t+1 \geq 3$ ungerade ist definiert durch die Codierungsregel

$$\varphi : \mathcal{A} \to \mathcal{A}^n, \qquad b \mapsto bb \cdots b.$$

Dieser Code besitzt nur $|\mathcal{A}|$ Codewörter. Die Minimaldistanz ist n und wir können t Fehler korrigieren: Wir decodieren ein Wort r zu dem am häufigsten vorkommenden Zeichen. Für $n = 3$ werden die Wörter abb, bab, bba mit $a \neq b$ zu bbb decodiert. Das entsprechende Informationswort ist also b.

1.2 Eigenschaften linearer Codes

Im Rest des Skriptes beschäftigen wir uns nur mit linearen Codes (Definition 1.2.1). Als Alphabet wählen wir immer einen endlichen Körper $\mathbb{F}_q$ mit $q = p^s$ Elementen, wobei p eine Primzahl ist. (Siehe Abschnitt 2.) Möchte man binäre Daten codieren, bietet sich das Alphabet $\mathbb{F}_2 = \{0, 1\}$ an.

Definition 1.2.1 Ein *linearer (n,k)-Code* $\mathcal{C}$ über $\mathbb{F}_q$ ist ein k-dimensionaler $\mathbb{F}_q$-Untervektorraum von $\mathbb{F}_q^n$. Hierbei ist k die *Dimension* und n die *Länge* des Codes.

Ein Code mit Dimension k, Länge n und Minimaldistanz d heißt (n, k, d)-Code.

Das *Gewicht* $w(v)$ eines Wortes $v \in \mathbb{F}_q^n$ ist definiert als $w(v) = d(v, 0)$. Für einen linearen Code $\mathcal{C}$ ist die Minimaldistanz gleich dem *Minimalgewicht* definiert als

$$d_{\min}(\mathcal{C}) = \min_{c \in \mathcal{C} \setminus \{0\}} w(c).$$

Dies folgt aus der Beobachtung $d(c^1, c^2) = d(c^1 - c^2, 0) = w(c^1 - c^2)$ für $c^1, c^2 \in \mathcal{C}$.

Wir beschäftigen uns im Weiteren nur noch mit linearen Codes und werden daher das Adjektiv "linear" weglassen.

Achtung: Wir schreiben Vektoren $y \in \mathbb{F}_q^n$ als **Zeilenvektoren** $y = (y_0, \ldots, y_{n-1})$. Dies ist in der Codierungstheorie üblich, entspricht aber nicht der Konvention aus der Vorlesung Lineare Algebra.

Definition 1.2.2 Sei $\mathcal{C}$ ein (n, k)-Code über $\mathbb{F}_q$. Eine *Erzeugermatrix* von $\mathcal{C}$ ist eine Matrix $G \in M_{k,n}(\mathbb{F}_q)$ deren Zeilen eine Basis von $\mathcal{C}$ bilden.

Eine Erzeugermatrix ist *in Standardform*, wenn sie von der Gestalt

$$G = (I_k | A)$$

mit $A \in M_{k,n-k}(\mathbb{F}_q)$ ist. Hierbei ist I_k die $k \times k$-Einheitsmatrix.

Eine Erzeugermatrix G eines Codes definiert eine injektive lineare Abbildung

$$\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^n, \qquad v \mapsto c = vG.$$

Diese Abbildung definiert also eine Codierungsregel. Ist die Matrix G in Standardform, dann ist die Codierung sehr einfach. Sei $c = (c_0, \ldots, c_{n-1}) \in \mathcal{C}$ ein Codewort. Dann besteht das entsprechende Informationswort $v = (c_0, \ldots, c_{k-1}) \in \mathbb{F}_q^k$ aus den ersten k Symbolen. Die übrigen Symbole heißen (wie beim ISBN-Code) *Prüfsymbole*.

Eine Matrix $G \in M_{k,n}(\mathbb{F}_q)$ ist genau dann die Erzeugermatrix eines Codes, wenn der Rang von G maximal, also k, ist. Dies ist genau dann der Fall, wenn die Zeilen von G linear unabhängig sind.

Beispiel 1.2.3 (a) Der Wiederholungscode aus Beispiel 1.1.8 mit Alphabet $\mathbb{F}_2$ ist ein linearer (n,1,n)-Code mit Erzeugermatrix

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}.$$

Diese Matrix ist in Standardform.

(b) Wir wählen das Alphabet $\mathbb{F}_2 = \{0, 1\}$ und betrachten die Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \in M_{4,7}(\mathbb{F}_2).$$

Die Matrix G ist in Standardform und definiert deswegen einen $(7,4)$-Code. Die Zeilenvektoren c^0, c^1, c^2, c^3 der Matrix bilden eine Basis des Codes. Die Codierungsregel ist

$$\varphi : \mathbb{F}_2^4 \to \mathbb{F}_2^7, v = (v_0, v_1, v_2, v_3) \mapsto vG = v_0c^0 + v_1c^1 + v_2c^2 + v_3c^3.$$

Sei $\mathcal{C}$ ein (n,k)-Code über $\mathbb{F}_q$ mit Erzeugermatrix G. Wir betrachten einen beliebigen Vektor $y \in \mathbb{F}_q^n$ und fragen uns, ob $y \in \mathcal{C}$ ist. Da $\mathcal{C}$ ein k-dimensionaler Untervektorraum von $\mathbb{F}_q^n$ ist, kann $\mathcal{C}$ als Lösungsmenge von $n-k$ linearen Gleichungen beschrieben werden. Dies motiviert folgende Definition.

Definition 1.2.4 Sei $\mathcal{C}$ ein (n,k)-Code über $\mathbb{F}_q$. Eine *Prüfmatrix* von $\mathcal{C}$ ist eine Matrix $H \in M_{n-k,n}(\mathbb{F}_q)$ von Rang $n-k$, sodass

$$Hc^t = 0, \qquad \text{für alle } c \in \mathcal{C}. \tag{1.2}$$

Beispiel 1.2.5 Wie im Beispiel 1.1.8 definiert man den $(n,1)$- Wiederholungscode über $\mathbb{F}_q$. Eine Prüfmatrix ist

$$H = \begin{pmatrix} -1 & 1 & & & \\ -1 & & 1 & & \\ \vdots & & & \ddots & \\ -1 & & & & 1 \end{pmatrix}.$$

Das Gleichungssystem $Hc^t = 0$ besteht aus den Prüfgleichungen $c_0 = c_i$ für $i = 1, \ldots, n-1$. Dies entspricht die Tatsache, dass alle Koeffizienten eines Codeworts gleich sind.

Lemma 1.2.6 *Die Bedingung (1.2) ist äquivalent zu*

$$G \cdot H^t = (0). \tag{1.3}$$

Beweis: Wir schreiben c^i für die i-te Zeile der Erzeugermatrix G von $\mathcal{C}$. Die Bedingung (1.3) ist äquivalent zu $c^iH^t = 0$ für $i = 0, \ldots, k-1$. Transponieren dieser Gleichung liefert $H(c^i)^t = 0$. Da $c^i \in \mathcal{C}$ ein Codewort ist, folgt (1.3) aus (1.2). Die Umkehrung folgt ebenfalls: Wegen der Linearität reicht es (1.2) für die Basis $(c^0, \ldots, c^{k-1})$ von $\mathcal{C}$ zu überprüfen. □

Lemma 1.2.7 *Sei $\mathcal{C}$ ein (n,k)-Code mit Erzeugermatrix $G = (I_k|A)$ in Standardform. Dann ist*

$$H = \left(-A^t | I_{n-k}\right)$$

eine Prüfmatrix von $\mathcal{C}$.

Beweis: Die Matrix H besitzt Rang $n-k$. Es gilt, dass

$$G \cdot H^t = \begin{pmatrix} I_k & A \end{pmatrix} \begin{pmatrix} -A \\ I_{n-k} \end{pmatrix} = (-A + A) = (0).$$

Das Lemma folgt also aus Lemma 1.2.6. □

Beispiel 1.2.8 (a) Für den $(7,4)$-Code aus Beispiel 1.2.3.(b) finden wir als Prüfmatrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

(b) Nicht jeder Code besitzt eine Erzeugermatrix in Standardform. Die Matrix

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \in M_{2,4}(\mathbb{F}_2)$$

definiert einen $(4,2)$-Code $\mathcal{C}$. Die Wörter dieses Codes sind $(0,0,0,0), (1,1,0,0)$, $(0,0,1,1), (1,1,1,1)$. Der Code besitzt also kein Wort $(1,0,a,b)$ mit $a,b \in \mathbb{F}_2$ und daher also auch keine Erzeugermatrix in Standardform.

Die Matrix G erfüllt $G \cdot G^t = (0)$. Also ist G auch eine Prüfmatrix des Codes. Solche Codes heißen selbstdual, siehe Abschnitt 1.6.

1.3 Die Minimaldistanz

Ein Ziel der Codierungstheorie ist es, "gute" Codes zu konstruieren. Beispielsweise möchte man für gegebenes (n,k) einen Code mit einer großen Minimaldistanz konstruieren. Solche Codes können möglichst viele Fehler korrigieren (Lemma 1.1.6). Der folgende Satz liefert eine obere Schranke für $d_{\min}$ in Termen von n und k. Reed–Solomon-Codes, die wir in Abschnitt 3 definieren, nehmen diese Schranke an (Lemma 3.1.2).

Satz 1.3.1 (Singletonschranke) *Sei $\mathcal{C}$ ein (n,k)-Code. Dann gilt*

$$d_{\min}(\mathcal{C}) \leq n + 1 - k.$$

Beweis: Sei $d = d_{\min}(\mathcal{C})$. Wir betrachten die Projektion

$$\psi : \mathbb{F}_q^n \to \mathbb{F}_q^{n+1-d}, \qquad (c_0, \ldots, c_{n-1}) \mapsto (c_0, \ldots, c_{n-d}).$$

Dies ist eine lineare Abbildung.

Aus der Definition der Minimaldistanz folgt, dass zwei verschiedene Codewörter sich an mindestens d Stellen unterscheiden. Die Einschränkung

$$\psi\big|_{\mathcal{C}} : \mathcal{C} \to \mathbb{F}_q^{n+1-d}$$

ist daher injektiv und es folgt, dass

$$k = \dim_{\mathbb{F}_q} \mathcal{C} \leq \dim_{\mathbb{F}_q} \mathbb{F}_q^{n+1-d} = n + 1 - d.$$

Hieraus folgt die Aussage des Satzes. □

Bemerkung 1.3.2 Ein Code mit $d_{\min} = n + 1 - k$ heißt *MDS-Code*. Dies ist eine Abbkürzung für *maximum distance separable*. Bei solche Codes sind die Codewörter maximal weit voneinander entfernt.

Im Allgemeinen ist es schwer die Minimaldistanz eines Codes zu bestimmen. Der folgende Satz gibt ein Kriterium in Termen der Prüfmatrix.

Satz 1.3.3 *Sei $\mathcal{C}$ ein (n,k)-Code mit Prüfmatrix H. Dann ist die Minimaldistanz $d_{\min}(\mathcal{C})$ die minimale Anzahl linear abhängiger Spalten von H.*

Beweis: Wir schreiben $s_j \in \mathbb{F}_q^k$ für die j-te Spalte von H. Seien $s_{j_1}, \ldots, s_{j_d}$ linear abhängige Spalten der Prüfmatrix H. Dann existieren $c_{j_1}, \ldots, c_{j_d} \in \mathbb{F}_q$, die nicht alle Null sind, sodass

$$c_{j_1} s_{j_1} + \cdots + c_{j_d} s_{j_d} = 0.$$

(Dies ist die Definition der linearen Abhängigkeit.) Für $\ell \neq j_i$ setzen wir $c_\ell = 0$. Dann erfüllt $c = (c_0, \ldots, c_{n-1})$ die Prüfgleichung $H \cdot c^t = 0$, also ist $c \in \mathcal{C}$. Aus $w(c) = d$ folgt, dass $d_{\min}(\mathcal{C}) \leq d$.

Ist umgekehrt $c \in \mathcal{C}$ ein Vektor vom Gewicht $w(c) = d$, dann gilt $H \cdot c^t = 0$, also sind die d Spalten s_j von H mit $c_j \neq 0$ linear abhängig. Die Aussage des Lemmas folgt. □

Beispiel 1.3.4 Der $(7,4)$-Code aus Beispiel 1.2.3.(b) besitzt Minimaldistanz 3. Beispielsweise gilt

$$s_1 + s_5 + s_6 = 0,$$

wobei s_j die j-te Spalte von H ist. Außerdem sind keine zwei Spalten gleich.

1.4 Syndromdecodieren

In diesem Abschnitt besprechen wir einen ersten Decodieralgorithmus.

Wir haben ein Wort r empfangen. Sei c das zugehörige Codewort. Das *Fehlerwort* ist definiert als

$$e = r - c.$$

Die *Fehlerstellen* $I = \{0 \leq i \leq n-1 \mid c_i \neq r_i\}$ sind genau die Stellen mit $e_i = r_i - c_i \neq 0$. Wir nehmen an, dass $t := w(e) \leq \lfloor (d-1)/2 \rfloor$ ist. Lemma 1.1.6 sagt, dass wir in diesem Fall dem Wort r eindeutig das Codewort c zuordnen können: Es ist das einzige Codewort mit $d(r,c) \leq \lfloor (d-1)/2 \rfloor$. Existiert ein solches Codewort nicht, dann enthält r mehr als $\lfloor (d-1)/2 \rfloor$ Fehler.

Sei $\mathcal{C} \subset \mathbb{F}_q^n$ ein (n,k,d)-Code mit Prüfmatrix H. Als Untervektorraum ist $\mathcal{C} < \mathbb{F}_q^n$ insbesondere eine Untergruppe. Wir betrachten die Nebenklassen von $\mathcal{C} < \mathbb{F}_q^n$. Diese kann man auch als Äquivalenzklassen der Äquivalenzrelation

$$x \sim y \qquad :\Leftrightarrow \qquad y - x \in \mathcal{C}$$

auffassen Die Linksnebenklasse von $x \in \mathbb{F}_q^n$ ist

$$x + \mathcal{C} = \{x + c \mid c \in \mathcal{C}\}.$$

Das folgende Lemma folgt direkt aus den bekannten Eigenschaften von Nebenklassen ([1, Bemerkung 1.8.2, Satz 1.8.3]).

Lemma 1.4.1 *(a) Der Vektorraum $\mathbb{F}_q^n$ ist die disjunkte Vereinigung von Linksnebenklassen.*

(b) Die Anzahl der Elemente von $x+\mathcal{C}$ hängt nicht von x ab, d.h. $|x+\mathcal{C}| = |\mathcal{C}|$.

Definition 1.4.2 Für $x \in \mathbb{F}_q^n$ heißt

$$s(x) := Hx^t \in \mathbb{F}_q^{n-k}$$

das *Syndrom* von x.

Die Codewörter sind durch $Hc^t = 0$ charakterisiert. Offensichtlich gilt also $x \sim y$ genau dann, wenn $Hx^t = Hy^t$. Die Linksnebenklassen entsprechen den Syndromen. Die Syndrome sind Spaltenvektoren in $\mathbb{F}_q^{n-k}$. Es gibt daher insgesamt q^{n-k} Syndrome.

Definition 1.4.3 Ein Element $y \in x+\mathcal{C}$ minimalen Gewichts in seiner Nebenklasse heißt *Nebenklassenführer*.

Algorithmus 1.4.4 (Syndromdecodieren) *Input*: Ein Wort r. *Output*: Ein Codewort c mit $d(r,c)$ minimal.

(I) (*Vorbereitung*) Wir erstellen eine Liste der Syndrome und der zugehörigen Nebenklassenführer. Enthält die Nebenklasse mehrere Wörter mit minimalem Gewicht, wählen wir zufällig eines aus. (In den Beispielen listen wir allerding immer alle auf.)

(II) (*Decodierung*) Wir haben einen Vektor r empfangen. Wir berechnen das Syndrom s. Sei e der Nebenklassenführer des Syndroms s. Dann ist $c = r - e$ das gesuchte Codewort.

Seien r, e, c wie in der Beschreibung des Algorithmus. Die Wörter r und e haben das gleiche Syndrom. Also ist

$$s(c) = s(r-e) = H(r-e)^t = Hr^t - He^t = 0.$$

Es folgt, dass c immer ein Codewort ist. Die möglichen Fehlerwörter sind die verschiedenen Vektoren in der Nebenklasse des Syndroms $s(r)$. Das Wort e besitzt minimales Gewicht in seiner Nebenklasse, also decodieren wir r zu einem Codewort c mit $d(c,r) = d(0,e) = w(e)$ minimal.

Beispiel 1.4.5 Wir betrachten den $(6,3)$-Code $\mathcal{C}$ über $\mathbb{F}_2$ gegeben durch die Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Mit Lemma 1.2.7 finden wir die Prüfmatrix

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Es folgt, dass $d_{\min}(\mathcal{C}) = 3$ und der Code kann einen Fehler korrigieren.

Wir finden folgende Nebenklassenführer. Hierbei bezeichnet e_j den j-ten Standardbasisvektor in $\mathbb{F}_2^6$. Die Syndrome sind Spaltenvektoren. Aus Platzgründen listen wir die entsprechenden Zeilenvektoren auf.

Syndrom^t	Nebenklassenführer
$(0,0,0)$	0
$(0,0,1)$	e_6
$(0,1,0)$	e_5
$(0,1,1)$	e_1
$(1,0,0)$	e_4
$(1,0,1)$	e_2
$(1,1,0)$	e_3
$(1,1,1)$	$e_1+e_4, e_2+e_5, e_3+e_6$.

Die Zeilen 2–7 der Tabelle sind leicht zu berechnen: Das Syndrom gehörig zu e_i entspricht der i-ten Spalte der Prüfmatrix H. Das letzte Syndrom besitzt keinen eindeutigen Nebenklassenführer.

Wir haben das Wort $r = (1,1,1,1,0,0)$ empfangen. Das Syndrom ist $s(r) = Hr^t = (1,0,0)^t$. Der entsprechende Nebenklassenführer ist e_4, also ist

$$c = r - e_4 = (1,1,1,0,0,0).$$

Dies ist das einzige Codewort, dass sich nur an einer Stelle von r unterscheidet.

Das empfangene Wort $\tilde{r} = (0,0,0,1,1,1)$ mit Syndrom $Hr^t = (1,1,1)^t$ können wir nicht eindeutig einem Codewort zuordnen. Es existiert kein Codewort, dass sich nur an einer Stelle von $\tilde{r}$ unterscheidet. Die Codewörter $r-(e_1+e_4) = (1,0,0,0,1,1), r-(e_2+e_5) = (0,1,0,1,0,1), r-(e_3+e_6) = (0,0,1,1,1,0)$ unterscheiden sich alle drei von r an 2 Stellen.

Satz 1.4.6 *Sei $\mathcal{C}$ ein (n,k)-Code. Der Code ist genau dann t-fehlerkorrigierend, wenn alle Wörter vom Gewicht t auch Nebenklassenführer von verschiedenen Nebenklassen sind.*

Beweis: "$\Rightarrow$" Wir nehmen an, dass $\mathcal{C}$ alle Fehlermuster vom Gewicht t korrigieren kann. Dann gilt, dass $d_{\min}(\mathcal{C}) \geq 2t+1$ ist (Lemma 1.1.6). Wir nehmen an, dass zwei verschiedene Wörter x und y mit $w(x) \leq t$ und $w(y) \leq t$ in der gleichen Nebenklasse existieren. Dann ist $c = x - y$ ein Codewort vom Gewicht $w(c) \leq 2t$. Dies liefert einen Widerspruch.

"$\Leftarrow$" Wir nehmen an, dass alle Wörter vom Gewicht kleiner gleich t Nebenklassenführer sind, aber dass zwei verschiedene Codewörter c^1, c^2 mit $d(c^1, c^2) =$

$w(c^1 - c^2) \leq 2t$ existieren. Dann existiert ein Wort y mit $d(y, c^i) \leq t$ für $i = 1, 2$. Wir schreiben $y = c^1 + e^1$ und $y = c^2 + e^2$.

Die Fehlervektoren e^i haben nach Annahme also Gewicht $w(e^i) = d(y, c^i) \leq t$. Da c^i ein Codewort ist, gilt

$$s(e^i) = s(c^i) + s(e^i) = s(c^i + e^i) = s(y).$$

Die Wörter e^i sind also beide Wörter vom Gewicht kleiner gleich t und liegen in der gleichen Nebenklasse. Dies widerspricht der Annahme. □

Beim Code aus Beispiel 1.4.5 ist jedes Wort von Gewicht kleiner gleich 1 ein Nebenklassenführer. In der Tat ist dieser Code 1-fehlerkorrigierend. Ein t-fehlerkorrigierender Code kann manchmal einige Fehlermuster von größerem Gewicht korrigieren. Dies illustriert das folgende Beispiel.

Beispiel 1.4.7 Wir betrachten den binären Code $\mathcal{C}$ mit Prüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in M_{5,7}(\mathbb{F}_2).$$

Die Spalten s_i von H erfüllen $s_1 + s_2 + s_6 + s_7 = 0$, also ist $d_{\min}(\mathcal{C}) \leq 4$. Man sieht leicht, dass keine drei Spalten von H linear abhängig sind, also ist $d_{\min}(\mathcal{C}) = 4$. Der Code ist also 1-fehlerkorrigierend.

Wir berechnen einige der Nebenklassenführer. Hierbei bezeichnen wir die Standardbasisvektoren von $\mathbb{F}_2^7$ mit e_i.

Syndrom^t	Nebenklassenführer
$(0,0,0,0,0)$	0
$(0,0,0,0,1)$	e_7
$(0,0,0,1,0)$	e_6
$(0,0,0,1,1)$	$e_1 + e_2, e_6 + e_7$
$(0,0,1,0,0)$	e_5
$(0,0,1,0,1)$	$e_5 + e_7$
$\vdots$	$\vdots$

Zum Syndrom $(0,0,0,1,1)^t$ existieren zwei verschiedene Nebenklassenführer $e_1 + e_2$ und $e_6 + e_7$. Zum Syndrom $(0,0,1,0,1)^t$ ist $e_5 + e_7$ der einzige Nebenklassenführer. Dies bedeutet, dass wir das Fehlermuster $e_5 + e_7$ eindeutig korrigieren können. Die Fehlermuster $e_1 + e_2$ und $e_6 + e_7$ können wir nicht eindeutig korrigieren.

1.5 Hamming-Codes

Sei $\mathcal{C}$ ein t-fehlerkorrigierender Code der Dimension n. Damit ein solcher Code möglichst viel Information verschicken kann, sollten die Wörter $y \in \mathbb{F}_q^n$ alle höchstens Hamming-Distanz t von einem Codewort haben.

Definition 1.5.1 Ein Code $\mathcal{C}$ heißt *perfekt*, wenn eine Zahl t existiert, sodass für jedes $y \in \mathbb{F}_q^n$ genau ein Codewort $c \in \mathcal{C}$ mit $d(y,c) \leq t$ existiert.

Satz 1.4.6 impliziert, dass die Nebenklassenführer eines perfekten Codes genau die Wörter vom Gewicht kleiner gleich t sind. In Abschnitt 1.4 haben wir Beispiele nicht-perfekter Codes gesehen. In den Beispielen 1.4.5 und 1.4.7 existieren Nebenklassenführer von Gewicht 2, aber die Codes sind nur 1-fehlerkorrigierend.

Aus dieser Beobachtung leiten wir folgende Schranke ab. Diese Schranke heißt manchmal auch die Kugelpackungsschranke.

Satz 1.5.2 (Hamming-Schranke) *Sei $\mathcal{C}$ ein (n,k)-Code über $\mathbb{F}_q$, der t-fehlerkorrigierend ist.*

(a) Es gilt

$$\sum_{j=0}^{t} (q-1)^j \binom{n}{j} \leq q^{n-k}. \tag{1.4}$$

(b) Ein Code ist genau dann perfekt, wenn Gleichheit in (a) gilt.

Beweis: Die Anzahl der Wörter vom Gewicht kleiner gleich t in $\mathbb{F}_q^n$ ist

$$1 + (q-1)\binom{n}{1} + (q-1)^2\binom{n}{2} + \cdots + (q-1)^t\binom{n}{t}.$$

In einem t-fehlerkorrigierenden Code sind alle Wörter vom Gewicht t Nebenklassenführer (Satz 1.4.6). Die Anzahl der Nebenklassen ist die Anzahl der Syndrome, also q^{n-k}. Dies liefert die Schranke aus (a). Aussage (b) folgt direkt aus (a) und Definition 1.5.1. □

Für $t = 1$ und $q = 2$ müssen perfekte Codes

$$n + 1 = 2^{n-k}$$

erfüllen. Die Länge n soll also von der Form $2^m - 1$ sind. Solche Zahlen heißen *Mersenne-Zahlen*. Lösungen sind beispielsweise $(n,k) \in \{(3,1),(7,4)\}$. Beispiele von perfekten Codes mit $t = 1$ sind der $(3,1)$-Wiederholungscode und der $(7,4)$-Code aus Beispiel 1.2.8, wie das folgende Beispiel zeigt.

Beispiel 1.5.3 (a) Die folgende Tabelle listet die Nebenklassenführer des $(7,4)$-Codes auf. Die Prüfmatrix haben wir in Beispiel 1.2.8 berechnet.

Syndrom^t	Nebenklassenführer
$(0,0,0)$	$(0,0,0,0,0,0,0)$
$(1,1,0)$	$(1,0,0,0,0,0,0)$
$(0,1,1)$	$(0,1,0,0,0,0,0)$
$(1,0,1)$	$(0,0,1,0,0,0,0)$
$(1,1,1)$	$(0,0,0,1,0,0,0)$
$(1,0,0)$	$(0,0,0,0,1,0,0)$
$(0,1,0)$	$(0,0,0,0,0,1,0)$
$(0,0,1)$	$(0,0,0,0,0,0,1)$.

Wir sehen, dass die Nebenklassenführer genau die Wörter vom Gewicht kleiner gleich 1 sind. Der Code ist also perfekt.

(b) Sei $q = 2$ und $n = 2t + 1$ ungerade. Wir zeigen, dass der $(n, 1, n)$-Wiederholungscode über $\mathbb{F}_2$ aus Beispiel 1.2.3.(a) ein perfekter Code ist. Dieser Code kann t Fehler korrigieren.

Es gilt

$$\sum_{i=0}^{2t+1} \binom{n}{i} = (1+1)^n = 2^n.$$

Wegen $\binom{n}{i} = \binom{n}{n-i}$ gilt

$$\sum_{j=t+1}^{2t+1} \binom{n}{j} = \sum_{j=t+1}^{2t+1} \binom{n}{n-j} = \sum_{i=0}^{t} \binom{n}{i}.$$

In der letzen Gleichheit haben wir $i = n - j$ gesetzt. Wir schließen, dass

$$\sum_{i=0}^{t} \binom{n}{i} = \frac{1}{2}\left(\sum_{i=0}^{2t+1} \binom{n}{i}\right) = 2^{n-1}.$$

Der Code besitzt Dimension $k = 1$, also ist dieser Code perfekt.

Der $(7, 4)$-Code aus dem obigen Beispiel ist ein Beipiel eines Hamming-Codes, den wir nun einführen.

Definition 1.5.4 Sei H_m eine Matrix über $\mathbb{F}_2$ deren Spalten genau alle verschiedenen Vektoren in $\mathbb{F}_2^m \setminus \{0\}$ sind. Ein *m-Hamming-Code* über $\mathbb{F}_2$ ist ein Code mit Prüfmatrix H_m.

Die Länge eines m-Hamming-Codes ist $n = 2^m - 1$: Dies ist die Kardinalität von $\mathbb{F}_2^m \setminus \{0\}$. Der Rang von H_m ist m, also ist $k = n - m = 2^m - 1 - m$.

Die Minimaldistanz des Codes ist 3: Die Spalten von H_m sind paarweise verschieden, aber die Summe zweier verschiedener Spalten ist auch eine Spalte von H. Satz 1.3.3 impliziert, dass die Minimaldistanz des Codes 3 ist. Hamming-Codes können also $t = 1$ Fehler korrigieren. Wir schließen, dass wir Gleichheit in der Hamming-Schranke (1.4) haben. Der folgende Satz folgt hieraus.

Satz 1.5.5 *Hamming-Codes sind perfekte* 1*-fehlerkorrigierende Codes.*

1.6 Der duale Code

Auf dem Vektorraum $\mathbb{F}_q^n$ definieren wir das *Standardskalarprodukt* als

$$(v, w) = \sum_{i=0}^{n-1} v_i w_i \in \mathbb{F}_q.$$

Zwei Vektoren $v, w \in \mathbb{F}_q^n$ heißen *orthogonal*, wenn $(v, w) = 0$.

Das Skalarprodukt über einem endlichen Körper ist symmetrisch und bilinear, aber nicht positiv definit. Der Vektor $v = (1, 1, 0, \ldots, 0) \in \mathbb{F}_2^n$ ist nicht der Nullvektor. Es gilt aber $(v, v) = 1+1 = 0 \in \mathbb{F}_2$. Der Vektor v ist also orthogonal zu sich selbst.

Definition 1.6.1 Sei $\mathcal{C}$ ein (n, k)-Code. Der *duale Code* ist definiert als

$$\mathcal{C}^\perp = \{v \in \mathbb{F}_q^n \mid (c, v) = 0 \text{ für alle } c \in \mathcal{C}\}.$$

Ein Code mit $\mathcal{C} = \mathcal{C}^\perp$ heißt *selbstdual*.

Ein Beispiel eines selbstdualen Codes haben wir in Beispiel 1.2.8.(b) gesehen.

Satz 1.6.2 *Sei $\mathcal{C}$ ein (n, k)-Code mit Erzeugermatrix G und Prüfmatrix H.*

(a) Die Matrix H ist eine Erzeugermatrix und G ist eine Prüfmatrix des dualen Codes $\mathcal{C}^\perp$.

(b) Der duale Code ist ein $(n, n-k)$-Code.

(c) Es gilt $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Beweis: Ein Vektor $v \in \mathbb{F}_q^n$ ist genau dann ein Element des dualen Codes, wenn $G \cdot v^t = 0$, da die Zeilen der Erzeugermatrix eine Basis von $\mathcal{C}$ bilden. Die Elemente des dualen Codes $\mathcal{C}^\perp$ sind also die Prüfgleichungen. Die Zeilen der Prüfmatrix bilden daher eine Basis des dualen Codes. Dies zeigt, dass H eine Erzeugermatrix von $\mathcal{C}^\perp$ ist. Aus

$$(G \cdot H^t)^t = H \cdot G^t = (0)^t = (0)$$

folgt ebenfalls, dass G eine Prüfmatrix von $\mathcal{C}^\perp$ ist. Dies zeigt (a).

Aussage (b) folgt sofort aus (a), da $H \in M_{n-k,n}(\mathbb{F}_q)$ ist. Die Definition des dualen Codes impliziert, dass $\mathcal{C} \subset (\mathcal{C}^\perp)^\perp$. Die Gleicheit in Aussage (c) folgt aus Dimensionsgründen. □

Das folgende Korollar folgt direkt aus Satz 1.6.2.(a) und Lemma 1.2.6.

Korollar 1.6.3 *Sei $\mathcal{C}$ ein Code mit Erzeugermatrix G. Dann ist $\mathcal{C}$ genau dann selbstdual, wenn*

$$G \cdot G^t = (0).$$

Beispiel 1.6.4 (a) Sei $\mathcal{C}$ der $(7, 4)$-Code aus Beispiel 1.2.8. Der duale Code $\mathcal{C}^\perp$ ist ein $(7, 3)$-Code mit Erzeuger- und Prüfmatrix gegeben durch

$$G_{\mathcal{C}^\perp} = H_{\mathcal{C}} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

$$H_{\mathcal{C}^\perp} = G_{\mathcal{C}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Mit Satz 1.3.3 folgt, dass die Minimaldistanz des dualen Codes $d_{\min}(\mathcal{C}^\perp) = 4$ ist.

(b) Wir konstruieren einen selbstdualen Code. Ist $\mathcal{C} = \mathcal{C}^\perp$, dann erfüllt die Dimension k von $\mathcal{C}$ die Gleichung $n - k = k$, also ist $n = 2k$ gerade.

Wir betrachten die lineare Abbildung

$$\psi : \mathbb{F}_2^n \to \mathbb{F}_2^{n+1}, \qquad (y_0, \ldots, y_{n-1}) \mapsto (y_0, \ldots, y_{n-1}, y_n := \sum_{i=0}^{n-1} y_i).$$

Diese Abbildung hängt am Ende des Worts y ein Paritätsbit $y_n = w(y) \pmod 2$ an. Das Wort $\psi(y)$ besitzt also immer gerades Gewicht.

Sei $\mathcal{C}$ der $(7, 4)$-Code aus (a). Wir definieren $\tilde{\mathcal{C}} = \psi(\mathcal{C})$. Ein so konstruierter Code heißt *erweiterter Code*. Die lineare Abbildung ψ ist injektiv, also besitzen beiden Codes die gleiche Dimension. Es folgt, dass $\tilde{\mathcal{C}}$ ein $(8, 4)$-Code ist. Die Matrix

$$\tilde{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

ist eine Erzeugermatrix von $\tilde{\mathcal{C}}$.

Man überprüft, dass

$$\tilde{G} \cdot \tilde{G}^t = (0).$$

Es folgt, dass $\tilde{\mathcal{C}}$ ein selbstdualer Code ist.

Übungsaufgabe 1.6.5 Sei $\mathcal{C} \subset \mathbb{F}_2^n$ ein (n, k, d)-Code. Wir bezeichnen mit $\tilde{\mathcal{C}} = \psi(\mathcal{C})$ den erweiterten Code, wie in Beispiel 1.6.4.(b) definiert. Zeige, dass

$$\tilde{H} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ & & & 0 \\ & H & & \vdots \\ & & & 0 \end{pmatrix}$$

eine Prüfmatrix von $\tilde{\mathcal{C}}$ ist.

2 Endliche Körper

2.1 Definition und Eigenschaften

Ein *endlicher Körper* ist ein Körper mit endlich vielen Elementen.

Lemma 2.1.1 *(a) Der Ring $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn m eine Primzahl ist.*

(b) Sei $\mathbb{F}$ ein endlicher Körper. Dann existiert eine Primzahl p, sodass $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{F}$ ein Teilkörper ist.

(c) Die Kardinalität eines endlichen Körpers ist eine Primzahlpotenz.

Beweis: (a) Wir schreiben $\mathbb{Z}/m\mathbb{Z} = \{[0], \ldots, [m-1]\}$. Der Ring $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper, wenn alle Elemente $[a] \in \mathbb{Z}/m\mathbb{Z} \setminus \{0\}$ Einheiten sind, d.h. wenn ein $b \in \mathbb{Z}$ mit $a \cdot b \equiv 1 \pmod{m}$ existiert. Dies ist genau dann der Fall, wenn $\mathrm{ggT}(a, m) = 1$. Ist nämlich $\mathrm{ggT}(a, m) = 1$, dann existieren $x, y \in \mathbb{Z}$ mit $1 = xa + ym$ und $[y]$ ist die Inverse von a. Elemente a mit $\mathrm{ggT}(a, m) > 1$ sind offensichtlich nicht invertierbar.

Ist $m = p$ eine Primzahl, dann ist $\mathbb{Z}/p\mathbb{Z}^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ und $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ist ein Körper. Ist m keine Primzahl, dann existieren $c, d \neq \pm 1$ mit $m = c \cdot d$ und die Kardinalität von $\mathbb{Z}/m\mathbb{Z}^*$ ist echt kleiner als $m-1$. Wir schließen, dass $\mathbb{Z}/m\mathbb{Z}$ kein Körper ist. Alternativ kann man auch benutzen, dass $c \neq 0$ ein Nullteiler und deswegen nicht invertierbar ist. Dies zeigt (a).

(b) Sei $\mathbb{F}$ ein endlicher Körper. Wir wählen $m \geq 1$ minimal, sodass $m \cdot 1 = 0$. Da $\mathbb{F}$ nur endlich viele Elemente besitzt, existiert ein solches m. Es folgt, dass $\mathbb{Z}/m\mathbb{Z} \subset \mathbb{F}$ eine Teilmenge ist. Ist m keine Primzahl, dann existiert ein nicht-trivialer Nullteiler $c \in \mathbb{Z}/m\mathbb{Z}$. Wie im Beweis von (a) liefert dies einen Widerspruch. Aussage (b) folgt.

(c) Sei $\mathbb{F}$ ein endlicher Körper mit Teilkörper $\mathbb{F}_p \subset \mathbb{F}$. Dann ist $\mathbb{F}$ ein $\mathbb{F}_p$-Vektorraum. Hierbei ist die Skalarmultiplikation $\mathbb{F}_p \times \mathbb{F} \to \mathbb{F}$ eine Einschränkung der Multiplikation des Körpers $\mathbb{F}$.

Sei $s := \dim_{\mathbb{F}_p} \mathbb{F}$ und $e_1, \ldots, e_s$ eine Basis von $\mathbb{F}$ als $\mathbb{F}_p$-Vektorraum. Die Elemente von $\mathbb{F}$ lassen sich eindeutig als

$$\mathbb{F} = \{c_1 e_1 + \cdots + c_s e_s \mid c_i \in \mathbb{F}_p\}$$

darstellen. Es folgt, dass $|\mathbb{F}| = p^s$ ist. □

Definition 2.1.2 Sei $\mathbb{F}$ ein endlicher Körper. Der *Charakteristik* von $\mathbb{F}$ ist die Primzahl p, sodass ein Teilkörper $\mathbb{F}_p \subset \mathbb{F}$ existiert. (Bezeichnung Char($\mathbb{F}$).) Der Teilkörper $\mathbb{F}_p \subset \mathbb{F}$ heißt *Primkörper*.

Wir werden zeigen, dass für jede Primzahlpotenz $q = p^s$ ein Körper mit q Elementen existiert (Theorem 2.1.4). Außerdem zeigen wir, dass zwei endliche Körper mit gleicher Kardinalität isomorph sind. Diesen Körper mit q Elementen werden wir mit $\mathbb{F}_q$ bezeichnen. Wir beweisen zunächst ein einfaches Lemma. Die Aussage ist als "freshman's dream"bekannt.

Lemma 2.1.3 *Sei $\mathbb{F}$ ein Körper der Charakteristik $p > 0$. Dann gilt*

$$(\alpha + \beta)^p = \alpha^p + \beta^p, \qquad \text{für alle } \alpha, \beta \in \mathbb{F}.$$

Beweis: Sei $1 \leq i \leq p-1$. Dann ist

$$\binom{p}{i} = \frac{p!}{i!(p-1)!} = 0 \in \mathbb{F}_p \subset \mathbb{F}.$$

Hier haben wir benutzt, dass p den Zähler aber nicht den Nenner des Bruchs teilt. Die Aussage des Lemmas folgt also aus der binomischen Formel. □

Theorem 2.1.4 *Sei $q = p^s$ eine Primzahlpotenz.*

(a) Es existiert ein Körper $\mathbb{F}$ mit q Elementen.

(b) Die Elemente von $\mathbb{F}$ sind Nullstellen des Polynoms $f_q(x) := x^q - x$. Dieses Polynom zerfällt in Linearfaktoren über $\mathbb{F}$.

(c) Zwei Körper mit q Elementen sind isomorph.

Beweis: Wir beweisen zuerst (b). Sei $\mathbb{F}$ ein Körper mit q Elementen. Die multiplikative Gruppe $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ enthält $q-1$ Elemente. Die Ordnung eines Elements $\alpha \in \mathbb{F}^*$ ist also ein Teiler der Gruppenordnung $q-1$ ([1, Satz 1.8.5]). Insbesondere ist α eine Nullstelle von $x^{q-1} - 1$, also auch von $f_q(x) = x^q - x$. Das Element $0 \in \mathbb{F}$ ist ebenfalls eine Nullstelle dieses Polynoms. Das Polynom f_q von Grad q besitzt also q verschiedene Nullstellen in $\mathbb{F}$ und zerfällt daher über $\mathbb{F}$ in Linearfaktoren:

$$f_q(x) = \prod_{\alpha \in \mathbb{F}} (x - \alpha).$$

Wir beweisen nun die Existenz eines Körpers $\mathbb{F}$ mit q Elementen. Teil (b) impliziert, dass die Elemente von $\mathbb{F}$ genau die Nullstellen von f_q sind.

Wir behaupten, dass eine Körpererweiterung L von $\mathbb{F}_p$, in dem f_q in Linearfaktoren zerfällt, existiert. Sei $g_1 \in \mathbb{F}_p[x]$ ein irreduzibler Faktor von f_q von Grad echt größer als 1. In der Körpererweiterung $L_1 := \mathbb{F}_p[x]/(g_1)$ besitzt g_1 eine Nullstelle. Mit Induktion folgt nun die Existenz einer Körpererweiterung, in der f_q in Linearfaktoren zerfällt. (Siehe auch [2, Satz 5.4.4].)

Wir behaupten, dass f_q keine mehrfache Nullstellen in L besitzt. Ist $\alpha \in L$ eine mehrfache Nullstelle, dann ist α auch eine Nullstelle der formalen Ableitung $f_q'(x) = qx^{q-1} - 1$. Da $q = p^n = 0 \in \mathbb{F}_p$, gilt $f_q'(x) = qx^{q-1} - 1 = -1 \in L[x]$. Also besitzt f_q keine mehrfachen Nullstellen. Da f_q in $L[x]$ in Linearfaktoren zerfällt, besitzt f_q in L genau q Nullstellen.

Sei $F \subset L$ die Menge der Nullstellen von f_q, d.h.

$$F = \{\alpha \in L \mid \alpha^q = \alpha\}.$$

Wir behaupten, dass F ein Körper ist. Seien $\alpha, \beta \in F$ mit $\alpha \neq 0$. Es gilt

$$(\alpha\beta)^q = \alpha^q\beta^q, \quad (-\beta)^q = -\beta, \quad (1/\alpha)^q = 1/\alpha^q.$$

Also sind $\alpha \cdot \beta$, $-\beta$ und $1/\alpha$ auch in F.

Wir müssen zeigen, dass $\alpha + \beta \in F$ ist. Mit Induktion folgt aus Lemma 2.1.3, dass

$$(\alpha + \beta)^q = (\alpha^p + \beta^p)^{p^{n-1}} = \cdots = \alpha^q + \beta^q \in L.$$

Wir haben angenommen, dass $\alpha, \beta \in F$, also $\alpha^q = \alpha$ und $\beta^q = \beta$. Es folgt, dass $(\alpha + \beta)^q = \alpha + \beta$. Insbesondere ist $\alpha + \beta \in F$. Wir schließen, dass F ein Körper ist.

Aussage (c) folgt aus (b). □

Der folgende Satz beschreibt die Ordnung der Elemente in $\mathbb{F}_q^*$. Wir erinnern uns, dass die *Ordnung* eines Elements $\alpha \in \mathbb{F}_q^*$ die kleinste positive Zahl r mit $\alpha^r = 1$ ist. Man zeigt leicht, dass

$$\operatorname{ord}(\alpha^i) = \frac{\operatorname{ord}(\alpha)}{\operatorname{ggT}(i, \operatorname{ord}(\alpha))}. \tag{2.1}$$

Satz 2.1.5 *Die Gruppe $\mathbb{F}_q^*$ ist zyklisch, d.h. es existiert ein Element $\alpha \in \mathbb{F}_q^*$ mit Ordnung $q-1$.*

Beweis: Sei $\alpha \in \mathbb{F}_q^*$ ein Element maximaler Ordnung $m = \operatorname{ord}(\alpha)$. Sei $H \subset \mathbb{F}_q^*$ die Untergruppe der Elemente deren Ordnung ein Teiler von m ist. Die Elemente von H sind genau die Nullstellen des Polynoms $g_m(x) := x^m - 1$. Da $\alpha \in H$ ist, besitzt H mindestens $m = \operatorname{ord}(\alpha)$ Elemente, nämlich die Elemente von $\langle\alpha\rangle = \{\alpha, \alpha^2, \ldots, \alpha^m = 1\}$. Da g_m höchstens m Nullstellen besitzt, sind dies auch die einzige Nullstellen von g_m. Es folgt, dass $H = \langle\alpha\rangle$ zyklisch ist.

Wir behaupten, dass $\operatorname{ord}(\alpha) = m = q-1$ ist. Ist $m < q-1$, dann ist $H \subsetneq \mathbb{F}_q^*$ und es existiert ein Element $\beta \in \mathbb{F}_q^* \setminus H$. Da $\beta \notin H$, ist $\ell := \operatorname{ord}(\beta) \nmid m$, also ist $\operatorname{kgV}(\ell, m) > m$. Das Element $\gamma := \alpha\beta$ besitzt Ordnung $\operatorname{kgV}(\ell, m) > m$. Dies widerspricht der Wahl von m als maximaler Ordnung eines Elements in $\mathbb{F}_q^*$. Es folgt, dass $m = q-1$, also ist $\mathbb{F}_q^* = H = \langle\alpha\rangle$ zyklisch. □

Bemerkung 2.1.6 Sei $\alpha \in \mathbb{F}_q^*$ ein Element der Ordnung $q-1$ wie in Satz 2.1.5. Dann gilt $\mathbb{F}_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1} = 1\}$. Ist $q = p$ eine Primzahl, dann heißt α Primitivwurzel modulo p.

Sei β ein Element der Ordnung r. Die Anzahl der Elemente der Ordnung r in $\langle\beta\rangle$ ist $\varphi(r)$, wobei φ die Eulersche φ-Funktion ist. Wir schreiben $r = \prod_i p_i^{e_i}$, wobei die p_i paarweise verschiedene Primzahlen sind. Dann gilt

$$\varphi(r) = \prod_i \left(p_i^{e_i - 1}(p_i - 1)\right),$$

[2, Satz 2.7.5].

2.2 Das Minimalpolynom

Theorem 2.1.4 impliziert, dass jedes Element $\beta \in \mathbb{F}_q$ eine Nullstelle von $f_q(x) = x^q - x \in \mathbb{F}_p[x]$ ist. Dies war der wichtigste Schritt im Beweis der Existenz und Eindeutigkeit endlicher Körper. Im Algemeinen ist β auch die Nullstelle eines Polynoms kleineren Grades. Der folgende Definition ist [1, Def. 4.2.4] formuliert in unserer Situation.

Definition 2.2.1 Sei $\beta \in \mathbb{F}_{p^s}$. Das *Minimalpolynom* $f(x) := \min_{\mathbb{F}_p}(\beta)$ ist das normierte Polynom kleinsten Grades mit Koeffizienten in $\mathbb{F}_p$, sodass β eine Nullstelle von f ist.

Sei $f(x) = \min_{\mathbb{F}_p}(\beta)$, dann ist f irreduzibel, d.h. es existieren keine Polynome $g, h \in \mathbb{F}_p[x]$ mit $f = g \cdot h$ mit g, h Polynome echt kleineren Grades. Ist nämlich $f = g \cdot h$, dann ist $f(\beta) = g(\beta)h(\beta)$, also ist β eine Nullstelle von g oder h. Dies widerspricht der Wahl von f als Polynom kleinsten Grades mit β als Nullstelle.

In Definition 2.2.1 fordern wir, dass das Minimalpolynom normiert ist, d.h. führenden Term $x^{\mathrm{Grad}(f)}$ besitzt. Dies impliziert, dass das Minimalpolynom eindeutig ist ([1, Satz 4.2.3]).

Lemma 2.2.2 *Sei $\beta \in \mathbb{F}_q^*$. Dann gilt*

$$\min_{\mathbb{F}_p}(\beta) \mid f_q \in \mathbb{F}_p[x].$$

Beweis: Sei $\beta \in \mathbb{F}_q^*$ und $m(x) = \min_{\mathbb{F}_p}(\beta)$. Mit Hilfe der Division mit Rest für Polynome schreiben wir

$$f_q(x) = q(x)m(x) + r(x), \qquad \mathrm{Grad}(r) < \mathrm{Grad}(m).$$

Als Element von $\mathbb{F}_q$ ist β eine Nullstelle von f_q (Theorem 2.1.4.(b)). Es ist ebenfalls eine Nullstelle seines Minimalpolynoms $m(x)$. Es folgt, dass $r(\beta) = 0$. Da $\mathrm{Grad}(r) < \mathrm{Grad}(m)$ folgt aus Definition 2.2.1, dass $r = 0$ ist. □

Beispiel 2.2.3 Wir faktorisieren $f_{16}(x) = x^{16} - x \in \mathbb{F}_2[x]$ in Linearfaktoren und finden

$$x^{16} - x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Dies berechnet man beispielsweise in Maple mit dem Kommando `Factor` $x^{16}-x \pmod 2$. Die irreduziblen Faktoren von $f_{16}(x)$ sind die möglichen Minimalpolynome von Elementen von $\mathbb{F}_{16}$. Der Faktor x besitzt 0 als Nullstelle.

Im Rest des Beispiels berechnen wir die Ordnung der Nullstellen der übrigen irreduziblen Faktoren von $x^{16} - x$. Diese Nullstellen sind in $\mathbb{F}_{16}^* \simeq \mathbb{Z}/15\mathbb{Z}$ (Satz 2.1.5). Daher ist die Ordnung dieser Nullstellen ein Teiler von $q - 1 = 15$. Aus (2.1) folgt außerdem, dass $\mathbb{F}_{16}^*$ genau 1 Element der Ordnung 1, $\varphi(3) = 2$ Elemente der Ordnung 3, $\varphi(5) = 4$ Elemente der Ordnung 5 und $\varphi(15) = \varphi(3)\varphi(5) = 8$ Elemente der Ordnung 15 enthält. Das einzige Element der Ordnung 1 ist $\beta = 1$ mit Minimalpolynom $x + 1 = x - 1 \in \mathbb{F}_2[x]$.

Sei β ein Element mit Minimalpolynom $\min_{\mathbb{F}_2}(\beta) = x^4 + x^3 + x^2 + x + 1$. Dann ist

$$\beta^5 - 1 = (\beta - 1)(\beta^4 + \beta^3 + \beta^2 + \beta + 1) = 0.$$

Also besitzt β Ordnung 5. Ebenso zeigt man, dass die Nullstellen von $x^2 + x + 1$ Ordnung 3 besitzen. Die 8 Elemente der Ordnung 15 sind also die Nullstellen von $x^4 + x + 1$ und $x^4 + x^3 + 1$.

Sei $q = p^n$ und $\beta \in \mathbb{F}_q$. Mit $\mathbb{F}_p(\beta)$ bezeichnen wir den kleinsten Teilkörper von $\mathbb{F}_q$, der β enthält. Sei $g(x) = \min_{\mathbb{F}_p}(\beta)$. Dann ist

$$\mathbb{F}_p(\beta) \simeq \mathbb{F}_p[x]/(g(x)).$$

(Siehe Lemma [1, Lemma 4.2.5].) Konkret bedeutet dies, dass

$$\mathbb{F}_p(\beta) = \left\{ \sum_{i=0}^{d-1} c_i \beta^i \mid c_i \in \mathbb{F}_p \right\}. \tag{2.2}$$

Insbesondere ist $d := \mathrm{Grad}(g) = [\mathbb{F}_p(\beta) : \mathbb{F}_p]$ der Grad der Körpererweiterung. Zwei Elemente von $\mathbb{F}_p(\beta)$ multipliziert man mit Hilfe der üblichen Rechenregel. Mit Hilfe der Relation $g(\beta) = 0$ kann man das Produkt wieder in der Form (2.2) schreiben.

Lemma 2.2.4 *(a) Sei $\beta \in \mathbb{F}_{p^s}$. Es gilt $\mathbb{F}_p(\beta) = \mathbb{F}_{p^d}$ für ein $d \mid s$.*

(b) Es existiert genau dann einen Teilkörper $L \subset \mathbb{F}_{p^s}$ mit $L \simeq \mathbb{F}_{p^d}$, wenn $d \mid s$.

Beweis: Wir zeigen zuerst (b). Sei $L \subset \mathbb{F}_{p^s}$ ein Teilkörper. Der Gradsatz ([1, Theorem 4.2.10]) sagt, dass

$$[\mathbb{F}_{p^s} : \mathbb{F}_p] = [\mathbb{F}_{p^s} : L] \cdot [L : \mathbb{F}_p].$$

Es folgt, dass $d = [\mathbb{F}_p(\beta) : \mathbb{F}_p] \mid [\mathbb{F}_{p^s} : \mathbb{F}_p] = s$. Dies zeigt die Hinrichtung von (b).

Sei d ein Teiler von s. Dann ist $x^{p^d} - x$ ein Teiler von $x^{p^s} - x$ (Übungsaufgabe). Insbesondere zerfällt $x^{p^d} - x$ in $\mathbb{F}_{p^s}$ in Linearfaktoren. Wie im Beweis von Theorem 2.1.4 folgt, dass

$$\mathbb{F}_{p^d} \simeq \{\beta \in \mathbb{F}_{p^s} \mid \beta^{p^d} = \beta\}$$

ein Teilkörper von $\mathbb{F}_{p^s}$ ist. Dies zeigt die Rückrichtung von (b).

Sei $\beta \in \mathbb{F}_{p^s}$. Dann ist $\mathbb{F}_p \subset \mathbb{F}_p(\beta) \subset \mathbb{F}_{p^s}$ ein Teilkörper. Aussage (a) folgt daher aus (b). □

Definition 2.2.5 Ein Element $\alpha \in \mathbb{F}_{p^s}$ heißt *primitives Element*, falls $\mathbb{F}_{p^s} = \mathbb{F}_p(\alpha)$.

Lemma 2.2.4 impliziert, dass $\alpha \in \mathbb{F}_{p^s}$ genau dann primitiv ist, wenn $s = \mathrm{Grad}(\min_{\mathbb{F}_p}(\alpha))$. Ist $\alpha \in \mathbb{F}_{p^s}^*$ ein Element der Ordnung $p^s - 1$, dann ist α ein primitives Element, da α in keinem echten Teilkörper $\mathbb{F}_{p^d}$ von $\mathbb{F}_{p^s}$ enthalten ist.

Beispiel 2.2.6 Dies ist eine Fortsetzung von Beispiel 2.2.3. Wir wählen ein $\alpha \in \mathbb{F}_{16}$ mit Minimalpolynom $\min_{\mathbb{F}_2}(\alpha) = x^4 + x + 1$. Wir haben gesehen, dass $\mathrm{ord}(\alpha) = 15$. Alle Elemente von $\mathbb{F}_{16}^*$ lassen sich als α^i schreiben. Die Elemente α^i können wir ebenfalls als $c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3$ mit $c_i \in \mathbb{F}_2$ schreiben (wie in (2.2)).

Die folgende Tabelle gibt eine Übersetzung zwischen beiden Darstellungen:

i	α^i	$\mathrm{ord}(\alpha)$
0	1	1
1	α	15
2	α^2	15
3	α^3	5
4	$\alpha^4 = \alpha + 1$	15
5	$\alpha^2 + \alpha$	3
6	$\alpha^3 + \alpha^2$	5
7	$\alpha^3 + \alpha + 1$	15
8	$\alpha^2 + 1$	15
9	$\alpha^3 + \alpha$	5
10	$\alpha^2 + \alpha + 1$	3
11	$\alpha^3 + \alpha^2 + \alpha$	15
12	$\alpha^3 + \alpha^2 + \alpha + 1$	5
13	$\alpha^3 + \alpha^2 + 1$	15
14	$\alpha^3 + 1$	15.

Das Polynom $x^4 - x$ zerfällt in $\mathbb{F}_{16}$ in Linearfaktoren. Die Nullstellen sind 0 und die Elemente deren Ordnung ein Teiler von 3 ist:

$$x^4 - x = x(x-1)(x^2 + x + 1) = x(x-1)(x-\alpha^5)(x-\alpha^{10}).$$

Also ist

$$\mathbb{F}_4 \simeq \mathbb{F}_2[x]/(x^2 + x + 1) \simeq \mathbb{F}_2(\alpha^5) \subset \mathbb{F}_{16}.$$

Beispiel 2.2.7 Wir illustrieren wie man im Körper $\mathbb{F}_q$ rechnen kann. Wir wählen $q = 16$ und benutzen die Bezeichnung aus Beispiel 2.2.3.

Die Darstellung der Elemente von $\mathbb{F}_{16}$ als α^i ist hilfreich beim Multiplizieren von Elementen. Beispielsweise ist

$$1/\alpha^3 = \alpha^{-3} = \alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1.$$

Bei der Addition ist die Schreibweise als Linearkombination von $1, \alpha, \alpha^2, \alpha^3$ einfacher. Beispielsweise ist

$$\alpha^5 + \alpha^7 = (\alpha^2 + \alpha) + (\alpha^3 + \alpha + 1) = \alpha^3 + \alpha^2 + 1 = \alpha^{13}.$$

Mit Hilfe der Tabelle kann man leicht zwischen beiden Darstellungen hin und her wechseln. Wir betrachten das Polynom $f(x) = 1 + \alpha^2 x^4 + \alpha^{10} x^5$. Dann ist

$$\begin{aligned} f(\alpha^2) &= 1 + \alpha^{10} + \alpha^{20} = 1 + \alpha^{10} + \alpha^5 \\ &= 1 + (1 + \alpha + \alpha^2) + (\alpha + \alpha^2) = 0. \end{aligned}$$

2.3 Bestimmung von irreduziblen Polynomen

Um im Körper $\mathbb{F}_q$ zu rechnen, ist es hilfreich den Körper als $\mathbb{F}_q = \mathbb{F}_p(\beta)$ darzustellen (Beispiel 2.2.7). Ist $\mathbb{F}_q = \mathbb{F}_p(\beta)$, dann ist $\min_{\mathbb{F}_p}(\beta) \in \mathbb{F}_p[x]$ ein irreduzibles Polynom vom Grad s (Lemma 2.2.4). Aus der Existenz des Körpers $\mathbb{F}_{p^s}$ folgt also die Existenz eines irreduziblen Polynoms in $\mathbb{F}_p[x]$ von Grad s.

In Abschnitt 4.4 werden wir die Beschreibung der irreduziblen Polynome über $\mathbb{F}_q$ benötigen. Daher wählen wir in diesem Abschnitt $\mathbb{F}_q$ als Grundkörper.

Satz 2.3.1 *Sei $\beta \in \mathbb{F}_{q^s}$ und $g(x) = \min_{\mathbb{F}_q}(\beta)$. Wir schreiben $d = \mathrm{Grad}(g(x))$. Es gilt*

(a) $g(\beta^q) = 0$,

(b)

$$g(x) = \prod_{i=0}^{d-1} (x - \beta^{q^i}) \in \mathbb{F}_{q^s}[x].$$

Beweis: Sei $g(x) \in \mathbb{F}_q[x]$ wie in der Aussage des Satzes. Wir schreiben

$$g(x) = \sum_{i=0}^{d} c_i x^i.$$

Da $c_i \in \mathbb{F}_q$ gilt, dass $c_i^q = c_i$. Lemma 2.1.3 impliziert also, dass

$$0 = g(\beta)^q = \left(\sum_{i=0}^{d} c_i \beta^i \right)^q = \sum_{i=0}^{d} c_i \beta^{qi} = g(\beta^q).$$

Dies zeigt (a).

Aus (a) folgt direkt, dass β^{q^i} für alle i eine Nullstelle von g ist. Wir müssen zeigen, dass g keine weitere Nullstellen besitzt. Lemma 2.2.4.(b) zeigt, dass $\mathbb{F}_q(\beta) = \mathbb{F}_{q^d}$. Dies bedeutet, dass d die kleinste positive Zahl mit $\beta^{q^d} = \beta$ ist.

Behauptung: Die β^{q^i} für $i = 0, \ldots, d-1$ sind paarweise verschieden.

Um einem Widerspruch abzuleiten, nehmen wir an, dass $0 \leq i < j \leq d-1$ mit $\beta^{q^i} = \beta^{q^j}$ existieren. Dann gilt

$$0 = \beta^{q^j} - \beta^{q^i} = (\beta^{q^{j-i}} - \beta)^{q^i},$$

Lemma 2.1.3. Es folgt, dass $\beta^{q^{j-i}} = \beta$. Da $0 < j-i < d$ ist $j-i$ eine positive Zahl als d mit dieser Eigenschaft. Dies liefert einen Widerspruch und die Behauptung folgt.

Die Behauptung impliziert, dass β^{q^i} mit $i = 0, \ldots, d-1$ paarweise verschiedene Nullstellen von g sind. Die Zahl d war definiert als der Grad von g, also besitzt g keine weitere Nullstellen. Aussage (b) folgt. □

Beispiel 2.3.2 Sei $\alpha \in \mathbb{F}_{16}$ ein Element mit Minimalpolynom $x^4 + x + 1$ wie in Beispiel 2.2.6. Dann gilt

$$x^4 + x + 1 = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8) \in \mathbb{F}_{16}[x].$$

Wir berechnen das Minimalpolynom über $\mathbb{F}_2$ von $\beta := \alpha^7$. Es gilt

$$\beta^2 = \alpha^{14}, \quad \beta^{2^2} = \alpha^{28} = \alpha^{13}, \quad \beta^{2^3} = \alpha^{11}.$$

Es gilt, dass $\beta^{2^4} = \beta$, da $\beta \in \mathbb{F}_{16}$. Wir schließen

$$\min(\beta) = (x - \alpha^7)(x - \beta^{14})(x - \alpha^{13})(x - \alpha^{11}) = x^4 + x^3 + 1.$$

Der Beweis von Satz 2.3.1 liefert auch eine Beschreibung der irreduziblen Polynome in $\mathbb{F}_p[x]$.

Definition 2.3.3 Wir betrachten die Menge $X_s = \mathbb{Z}/(q^s - 1)\mathbb{Z}$. Sei $a \in X_s$ und m_a die kleinste positive Zahl, sodass

$$q^{m_a} a \equiv a \pmod{q^s - 1}.$$

Die *zyklotomische Nebenklasse* von a ist die Menge

$$C_a = \{a, qa, q^2 a, \ldots, q^{m_a - 1} a\} \subset X_s.$$

Wir wählen ein festes $\alpha \in \mathbb{F}_q^*$ der Ordnung $q^s - 1$. Wir definieren

$$M^{(a)} := \prod_{j=0}^{m_a - 1} (x - \alpha^{q^j a}).$$

Bemerke, dass $M^{(a)}$ nur von der zyklotomischen Nebenklasse C_a und nicht von der Wahl des Repräsentanten a abhängt.

Korollar 2.3.4 *(a) Die Polynome $M^{(a)} \in \mathbb{F}_q[x]$ sind irreduzibel.*

(b) Sei $g(x) \in \mathbb{F}_q[x]$ ein normiertes irreduzibles Polynom vom Grad $d \mid s$. Dann existiert ein a mit $g(x) = M^{(a)}(x)$.

Beweis: In Satz 2.3.1 haben wir gezeigt, dass $M^{(a)}(x)$ das Minimalpolynom von α^a ist. Insbesondere ist $M^{(a)}(x)$ irreduzibel. Dies zeigt (a).

Sei g wie in (b). Dann ist $L := \mathbb{F}_q[x]/(g) \simeq \mathbb{F}_{q^d}$. Da $d \mid s$, können wir L als Teilkörper von $\mathbb{F}_{q^s}$ auffassen (Lemma 2.2.4). In L, also auch in $\mathbb{F}_{q^s}$, besitzt das Polynom g eine Nullstelle β ([1, Lemma 4.2.5]). Es existiert ein a mit $\beta = \alpha^a$. Da g irreduzibel ist, folgt, dass

$$g(x) = \min_{\mathbb{F}_q}(\beta) = M^{(a)}.$$

□

Beispiel 2.3.5 Wir betrachten $q = 2$ und $q^s = 16$. Wie in den Beispielen 2.2.3, 2.2.6 und 2.3.2 wählen wir α als Nullstelle von $x^4 + x + 1$. Die folgende Tabelle listet die zyklotomischen Nebenklassen und die entsprechenden Polynome $M^{(a)}$ auf:

a	C_a	$M^{(a)}$
0	$\{0\}$	$x + 1$
1	$\{1, 2, 4, 8\}$	$x^4 + x + 1$
3	$\{3, 6, 12, 9\}$	$x^4 + x^3 + x^2 + x + 1$
5	$\{5, 10\}$	$x^2 + x + 1$
7	$\{7, 14, 13, 11\}$	$x^4 + x^3 + 1$

Die Berechnungen der Minimalpolynome $M^{(a)}$ haben wir in den vorhergehenden Beispielen schon gemacht.

Bemerkung 2.3.6 In diesem Abschnitt spielte die Abbildung

$$F : \mathbb{F}_{q^s} \to \mathbb{F}_{q^s}, \qquad x \mapsto x^q$$

eine wichtige Rolle. Diese Abbildung erfüllt $F(xy) = F(x)F(y)$ und $F(x+y) = F(x) + F(y)$ (Lemma 2.1.3). Dies bedeutet, dass F ein Ringhomomorphismus ist. Da F offensichtlich bijektiv ist, ist F sogar ein Ringisomorphismus von $\mathbb{F}_{q^s}$ mit sich selbst. Diese Abbildung heißt *q-Frobenius-Automorphismus*.

3 Reed–Solomon-Codes

Reed–Solomon-Codes sind eine Klasse viel benutzter Codes. Beispielsweise werden sie bei CD-Spielern und in QR-Codes benutzt.

3.1 Definition

Sei $q = p^s$ eine Primzahlpotenz und $\mathbb{F}_q$ der Körper mit q Elementen.

Ein *Auswertungsvektor in* $\mathbb{F}_q$ ist ein Vektor $a := (a_0, \ldots, a_{n-1})$, wobei $a_i \in \mathbb{F}_q$ paarweise verschieden sind. Bemerke, dass notwendigerweise $n \leq q$ ist. Wir bezeichnen mit $P_k = \{f \in \mathbb{F}_q[x] \mid \mathrm{Grad}_x(f) < k\}$ den k-dimensionalen Vektorraum der Polynome vom Grad echt kleiner als k. **Achtung**: k bezeichnet die Dimension von P_k als $\mathbb{F}_q$-Vektorraum und nicht den maximalen Grad der Polynome.

Im Folgenden werden wir immer annehmen, dass $k \leq n$ ist.

Definition 3.1.1 Ein *Reed-Solomon-Code* (kurz: RS-Code) ist das Bild der linearen Abbildung

$$\varphi : P_k \to \mathbb{F}_q^n, \qquad f \mapsto (f(a_i))_{i=0}^{n-1}. \tag{3.1}$$

Hierbei ist $k \leq n$ und $a := (a_i)_i$ ein Auswertungsvektor in $\mathbb{F}_q$.

Lemma 3.1.2 *Sei $k \leq n$. Ein RS-Code mit Parameter (n, k) ist ein $(n, k, n + 1 - k)$-Code. Insbesondere kann der Code $\lfloor (n-k)/2 \rfloor$ Fehler korrigieren.*

Beweis: Wir definieren den RS-Code $\mathcal{C}$ als das Bild einer Abbildung φ wie in (3.1). Als Bild einer linearen Abbildung ist $\mathcal{C}$ offensichtlich linear. Die Länge des Codes ist n, da $\mathcal{C} \subset \mathbb{F}_q^n$.

Ein Polynom $f \in P_k$ besitzt höchstens $\text{Grad}(f) \leq k-1$ Nullstellen. Ist $f \in \ker(\varphi)$, dann ist $f(a_i) = 0$ für $0 \leq i \leq n-1$ und f besitzt mindestens $n > k-1$ Nullstellen. Es folgt, dass f das Nullpolynom ist. Also ist φ injektiv und die Dimension des Codes ist $k = \dim_{\mathbb{F}_q} P_k$.

Sei $c := \varphi(f) = (c_0, \ldots, c_{n-1})$ ein Codewort. Dann ist $c_i = f(a_i)$. Da $f \in P_k$ höchstens $k-1$ Nullstellen besitzt, gilt $w(c) \geq n - (k-1) = n + 1 - k$. Also ist $d_{\min}(\mathcal{C}) \geq n + 1 - k$. Das Lemma folgt aus der Singleton-Schranke (Satz 1.3.1). □

Jedes Polynom $f \in P_k$ kann man als $f(x) = \sum_{i=0}^{k-1} b_i x^i$ schreiben. Wir wählen $\mathcal{B} = (1, x, \ldots, x^{k-1})$ als Basis von P_k. Bezüglich dieser Basis können wir f also als Vektor $(b_0, \ldots, b_{k-1})$ auffassen. Dies ist das Informationswort.

Die Abbildung φ aus Definition 3.1.1 ist eine Codierungsabbildung. Es folgt, dass die Matrix

$$G := M(\varphi) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ a_0^{k-1} & a_1^{k-1} & a_2^{k-1} & \cdots & a_{n-1}^{k-1} \end{pmatrix} \tag{3.2}$$

von φ eine Erzeugermatrix des RS-Codes ist.

In Definition 3.1.1 haben wir allgemeine RS-Codes definiert. In der Praxis benutzt man eine spezielle Unterklasse von RS-Codes, die wir in der nächsten Definition definieren. Ab jetzt werden wir immer nur solche RS-Codes betrachten. Wieso diese Codes zyklisch heißen, werden wir in Abschnitt 4 sehen.

Definition 3.1.3 Sei $n \mid (q-1)$. Ein *zyklischer RS-Code* $RS^{n,k}(\beta)$ ist ein RS-Code mit Auswertungsvektor $(1, \beta, \beta^2, \ldots, \beta^{n-1})$, wobei $\beta \in \mathbb{F}_q^*$ ein Element der Ordnung n ist.

In Satz 2.1.5 haben wir gesehen, dass $\mathbb{F}_q^*$ eine zyklische Gruppe der Ordnung $q-1$ ist. Diese Gruppe besitzt genau dann ein Element der Ordnung n, wenn $n \mid (q-1)$. Dies erklärt die Bedingung in der obigen Definition.

Beispiel 3.1.4 Sei $\mathbb{F}_{16}$ ein Körper mit 16 Elementen und $\alpha \in \mathbb{F}_{16}$ eine Nullstelle von $x^4 + x + 1$. In Beispiel 2.2.3 haben wir gesehen, dass α Ordnung 15 besitzt. Das Element $\beta := \alpha^3$ besitzt also Ordnung $n = 15/3 = 5$. Wir beschreiben den entsprechenden zyklischen RS-Code.

Wir wählen $k = 3$ und $(1, \beta := \alpha^3, \beta^2 = \alpha^6, \beta^3 = \alpha^9, \beta^4 = \alpha^{12})$ als Auswertungsvektor. Sei $\mathcal{C}$ der zugehörige zyklische RS-Code. Lemma 3.1.2 impliziert, dass $d_{\min}(\mathcal{C}) = n + 1 - k = 3$.

Sei φ wie in (3.1). Eine Basis von $\mathcal{C}$ über $\mathbb{F}_{16}$ ist

$$\begin{aligned} c^0 &:= \varphi(1) = (1,1,1,1,1), \\ c^1 &:= \varphi(x) = (1, \beta = \alpha^3, \beta^2 = \alpha^6, \beta^3 = \alpha^9, \beta^4 = \alpha^{12}), \\ c^2 &:= \varphi(x^2) = (1, \beta^2, \beta^4, \beta^6 = \alpha^3, \beta^8 = \alpha^9). \end{aligned}$$

Satz 3.1.5 *Sei $\mathcal{C} = RS^{n,k}(\beta)$ ein zyklischer RS-Code. Der Auswertungsvektor ist also $a_i = \beta^i, i = 0, \ldots, n-1$ und $\beta \in \mathbb{F}_q^*$ besitzt Ordnung n. Die Matrix*

$$\begin{aligned} H &= \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_0^2 & a_1^2 & a_2^2 & \cdots & a_{n-1}^2 \\ \vdots & \vdots & \vdots & & \vdots \\ a_0^{n-k} & a_1^{n-k} & a_2^{n-k} & \cdots & a_{n-1}^{n-k} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^2 & \cdots & (\beta^2)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{n-k} & \cdots & (\beta^{n-k})^{n-1} \end{pmatrix} \in M_{n-k,n}(\mathbb{F}_q) \end{aligned} \tag{3.3}$$

ist eine Prüfmatrix von $\mathcal{C}$.

Beweis: Behauptung 1: Die Matrix H besitzt Rang $n-k$.

Es ist offensichtlich, dass der Rang von H höchstens $n-k$ ist. Die Behauptung folgt daher, wenn wir eine invertierbare $(n-k) \times (n-k)$-Untermatrix $\tilde{H}$ von H konstruieren.

Wir betrachten die $(n-k) \times (n-k)$-Untermatrix $\tilde{H}$ von H, bestehend aus den ersten $n-k$ Spalten. Es gilt

$$\det(\tilde{H}) = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-k-1} \\ a_0^2 & a_1^2 & a_2^2 & \cdots & a_{n-k-1}^2 \\ \vdots & \vdots & \vdots & & \vdots \\ a_0^{n-k} & a_1^{n-k} & a_2^{n-k} & \cdots & a_{n-k-1}^{n-k} \end{vmatrix} =$$

$$a_0 \cdots a_{n-k-1} \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{n-k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ a_0^{n-k-1} & a_1^{n-k-1} & a_2^{n-k-1} & \cdots & a_{n-k-1}^{n-k-1}. \end{vmatrix}$$

Die letzte Determinante ist die Determinante der Transponierten einer Vandermonde-Matrix. Es folgt, dass

$$\det(\tilde{H}) = a_0 \cdots a_{n-k-1} \prod_{0 \le i < j \le n-k-1} (a_j - a_i).$$

Die Wahl der a_i impliziert, dass die a_i paarweise verschieden und ungleich Null sind. Es folgt, dass die Matrix $\tilde{H}$ invertierbar ist. Hieraus folgt Behauptung 1.

Behauptung 2: Sei G wie in (3.2). Dann gilt $G \cdot H^t = (0)$.

Der $(i+1, j)$-te Eintrag von $G \cdot H^t$ ist

$$\begin{pmatrix} a_0^i & a_1^i & \cdots & a_{n-1}^i \end{pmatrix} \begin{pmatrix} a_0^j \\ a_1^j \\ \vdots \\ a_{n-1}^j \end{pmatrix} = \sum_{s=0}^{n-1} a_s^{i+j}.$$

Wir haben $a_j = \beta^j$ gewählt. Also erhalten wir

$$\sum_{s=0}^{n-1} a_s^{i+j} = \sum_{s=0}^{n-1} (\beta^{i+j})^s.$$

Die Matrix $G \cdot H^t$ ist eine $k \times (n-k)$-Matrix, also ist $1 \leq (i+1) \leq k$ und $1 \leq j \leq n-k$. Es folgt, dass $1 \leq i+j \leq n-1$. Das Element β besitzt Ordnung n, also ist $(\beta^{i+j})^n = 1$ aber $\beta^{i+j} \neq 1$. Es folgt, dass

$$\sum_{s=0}^{n-1} (\beta^{i+j})^s = \frac{(\beta^{i+j})^n - 1}{\beta^{i+j} - 1} = 0.$$

Dies zeigt Behauptung 2. Der Satz folgt aus den beiden Behauptungen. □

3.2 Das Fehlerstellenpolynom

Im Rest des Kapitels beschreiben wir einen Algorithmus zum Decodieren von zyklischen RS-Codes. Der Algorithmus basiert auf dem euklidischen Algorithmus.

Sei $\beta \in \mathbb{F}_q^*$ ein Element der Ordnung n, insbesondere gilt $n \mid (q-1)$. Sei $\mathcal{C}$ der zyklische $(n, k, n+1-k)$-RS-Code mit Auswertungsvektor $(1, \beta, \beta^2, \ldots, \beta^{n-1})$. Dieser Code kann $t := \lfloor (n-k)/2 \rfloor$ Fehler korrigieren.

Sei $r = (r_0, \ldots, r_{n-1}) \in \mathbb{F}_q^n$ ein empfangenes Wort. Wir schreiben $r = c + e$, wobei $c = (c_i)$ das Codewort und $e = (e_i)$ das Fehlerwort ist. Wir nehmen an, dass $w(e) \leq t$. Wir können also den Fehler e korrigieren. Unser Ziel ist es, das Codewort c aus dem empfangenen Wort r zu berechnen. Der erste Schritt des Verfahrens ist die Berechnung der Fehlerstellen.

Definition 3.2.1 Die *Fehlerstellen* sind die Werte

$$I := \{0 \leq i \leq n-1 \mid e_i \neq 0\}.$$

Das Polynom

$$\Lambda(x) = \prod_{i \in I} (x - \beta^i) \in \mathbb{F}_q[x]$$

heißt *Fehlerstellenpolynom*. Wir schreiben $\tau = |I| = \mathrm{Grad}(\Lambda)$ für die Anzahl der Fehler.

Beispiel 3.2.2 Das Element $\beta := 2 \in \mathbb{F}_5^*$ besitzt Ordnung 4 und definiert den Auswertungvektor $(1, \beta = 2, \beta^2 = 4, \beta^3 = 3)$. Sei $\mathcal{C}$ der $(4, 2, 3)$-RS-Code mit diesem Auswertungsvektor.

Das Polynom $f(x) = 1 + x \in P_2$ definiert das Wort $c = (2, 3, 0, 4)$. Wir betrachten den Fehlervektor $e = (0, 0, 0, 1)$ und erhalten $r = c + e = (2, 3, 0, 0)$. Es ist $I = \{3\}$ und das Fehlerstellenpolynom ist

$$\Lambda(x) = (x - \beta^3) = (x - 3).$$

In Definition 1.4.2 haben wir das Syndrom von r als den Vektor $s(r) = Hr^t \in \mathbb{F}_q^{n-k}$ definiert. Die Prüfmatrix H erfüllt $Hc^t = 0$ für alle Codewörter c, also gilt auch

$$s(r) = Hr^t = H(c + e)^t = Hc^t + He^t = He^t.$$

Wir schreiben $s(r) = (S_1, \ldots, S_{n-k})$. Mit Hilfe der Prüfmatrix H aus Satz 3.1.5 finden wir für zyklische RS-Codes

$$S_i = \sum_{j=0}^{n-1} r_j \beta^{ij} = \sum_{j=0}^{n-1} e_j \beta^{ij}, \qquad i = 1, \ldots, n - k. \tag{3.4}$$

Der zweite Ausdruck ist hilfreich in Beweisen, aber nicht um die Syndrome zu berechnen, da e nicht bekannt ist.

Bemerkung 3.2.3 Die Formel (3.4) kann man sich leicht merken, indem man das Wort r als Polynom auffasst. Dazu bemerken wir, dass

$$\mathbb{F}_q^n \to P_n, \qquad r = (r_0, \ldots, r_{n-1}) \mapsto r(x) := \sum_{i=0}^{n-1} r_i x^i$$

ein Isomorphismus von $\mathbb{F}_q$-Vektorräumen ist. Identifizieren wir das Wort $r = (r_i)$ mit dem Polynom $r(x)$, dann können wir (3.4) auch als

$$S_i = r(\beta^i)$$

schreiben. Eine genauere Variante dieser Konstruktion beschreiben wir in Abschnitt 4.

Definition 3.2.4 Sei $r = (r_i) \in \mathbb{F}_q^n$ ein empfangenes Wort. Das Polynom

$$S(x) := \sum_{i=1}^{2t} S_i x^{2t-i} = \sum_{j=0}^{2t-1} S_{2t-j} x^j = S_{2t} + S_{2t-1} x + \cdots + S_1 x^{2t-1}$$

heißt *Syndrompolynom*.

Achtung: Bitte beachten Sie die Indizierung der Koeffizienten des Syndrompolynoms.

Nach Definition gilt $t = \lfloor (n-k)/2 \rfloor$, also $2t \leq n-k$. Dies bedeutet, dass alle im Syndrompolynom vorkommenden Syndrome in der Tat definiert sind. Um das Syndrompolynom zu bestimmen, braucht man nur die Syndrome S_i mit $1 \leq i \leq 2t$.

Beispiel 3.2.5 Wir berechnen das Syndrompolynom des Worts $r = (2, 3, 0, 0)$ aus Beispiel 3.2.2. Dazu fassen wir r als Polynom $r(x) = 2 + 3x$ auf. Der Code kann $t = 1$ Fehler korrifieren. Es gilt $S_1 = r(\beta) = r(2) = 3$ und $S_2 = r(\beta^2) = r(4) = 4$. Das Syndrompolynom ist

$$S = S_2 + S_1 x = 4 + 3x.$$

Aus der Tatsache, dass die Syndrome nicht alle Null sind, folgt, dass r kein Codewort ist. In Beispiel 3.2.2 hatten wir r gerade als Codewort mit $\tau = 1$ Fehler konstruiert, also ist dies keine Überrasschung.

Der folgende Satz bildet die Grundlage des Decodierverfahrens.

Satz 3.2.6 *Sei r ein empfangenes Wort mit höchstens $\tau \leq t = \lfloor (n-k)/2 \rfloor$ Fehlerstellen und sei S das entsprechende Syndrompolynom. Sei $\Lambda(x) = \sum_{i=0}^{\tau} \lambda_j x^j$ das Fehlerstellenpolynom und $S = \sum_{i=0}^{2t-1} S_{2t-i} x^i$ das Syndrompolynom. Wir schreiben*

$$\Lambda(x) S(x) = \sum_i \mu_i x^i.$$

Dann gilt $\mu_i = 0$ für $\tau \leq i \leq 2t-1$.

Satz 3.2.6 impliziert, dass ein Polynom $R \in \mathbb{F}_q[x]$ mit $\mathrm{Grad}(R) \leq \tau - 1$ existiert, sodass

$$\Lambda \cdot S \equiv R \pmod{x^{2t}}. \tag{3.5}$$

Diese Kongruenz ist bekannt als die *Schlüsselgleichung*. Das entsprechende Polynom R heißt *Fehlerauswertungspolynom*. Mit diesem Polynom kann man die Fehlerwerte berechnen. Dies besprechen wir im nächsten Abschnitt.

Beweis: Wir haben angenommen, dass das Gewicht $w(e)$ des Fehlerworts höchstens $t = \lfloor (n-k)/2 \rfloor$ ist. Also ist $\mathrm{Grad}(\Lambda) \leq t$ und $\mathrm{Grad}(\Lambda \cdot S) \leq t + (2t-1)$.

Die im Syndrompolynom enthaltenen Syndrome sind S_i mit $1 \leq i \leq 2t$. Einfachheitshalber setzen wir in diesem Beweis $S_i = 0$ falls $i \leq 0$ oder $i > 2t$.

Die Definition von μ_i impliziert, dass

$$\mu_i = \sum_{0 \leq j \leq \tau} (\lambda_j S_{2t-i+j}). \tag{3.6}$$

Um den Satz zu beweisen, betrachten wir die Koeffizienten μ_i für $\tau \leq i \leq 2t-1$. Aus den Ungleichungen $0 \leq j \leq \tau$ und $\tau \leq i \leq 2t-1$ folgt, dass $1 \leq 2t - i + j \leq$

$2t$. Alle Koeffizienten S_{2t-i+j}, die in der Summe (3.6) vorkommen, sind also tatsächlich Syndrome.

Mit (3.4) folgt, dass

$$\begin{aligned}\mu_i &= \sum_{j=0}^{\tau} \lambda_j \left(\sum_{\ell=0}^{n-1} e_\ell (\beta^\ell)^{2t+j-i} \right) \\ &= \sum_{\ell=0}^{n-1} e_\ell (\beta^\ell)^{2t-i} \left(\sum_{j=0}^{\tau} \lambda_j (\beta^\ell)^j \right) \\ &= \sum_{\ell=0}^{n-1} e_\ell (\beta^\ell)^{2t-i} \Lambda(\beta^\ell).\end{aligned}$$

Falls ℓ keine Fehlerstelle ist, ist $e_\ell = 0$. Ansonsten ist $\Lambda(\beta^\ell) = 0$. Wir schließen, dass $\mu_i = 0$ für $\tau \leq i \leq 2t-1$. □

Beispiel 3.2.7 (a) Dies ist eine Fortsetzung von Beispiel 3.2.5. Dort haben wir $\Lambda = x - 3$ und $S = 4 + 3x$ berechnet. Wir finden

$$\Lambda(x) \cdot S(x) = (x-3)(4+3x) = 3x^2 + 3.$$

Die Koeffizienten μ_i mit $1 = \tau \leq i \leq 2t-1 = 1$ dieses Polynoms verschwinden. Wir finden $R = 3$.

(b) Wir betrachten den selben Code aber haben diesmal das Wort $r = (2,2,3,1)$ empfangen, also $r(x) = 2+2x+3x^2+x^3$. Wir berechnen $S_1 = r(2) = 1$ und $S_2 = r(4) = 2$, also $S(x) = 2 + x$. Um die Fehlerstellen zu berechnen, betrachten wir $\Lambda(x) = x + a$. Es gilt

$$\Lambda(x) \cdot S(x) = x^2 + (2+a)x + 2a.$$

Ist Λ ein Fehlerstellenpolynom, dann muss der Koeffizient $2 + a$ von x in $\Lambda \cdot S$ verschwinden. Wir schließen, dass $a = -2$ und $\Lambda(x) = x - 2$. Das Fehlerauswertungspolynom ist $R(x) = 1$. Das Fehlerstellenpolynom Λ besitzt die Nullstelle $2 = \beta^1$. Die Fehlerstelle ist also $i = 1$.

Um den Fehlerwert e_1 zu berechnen, benutzen wir (3.4). Wir wissen, dass $i = 1$ die einzige Fehlerstelle ist. Daher gilt $S_i = e_1 \beta^{1 \cdot i}$. Wir finden $1 = S_1 = e_1 \cdot 2^1$ und schließen, dass $e_1 = 3$ ist. Das gesuchte Codewort ist

$$c = r - e = (2,2,3,1) - (0,3,0,0) = (2,4,3,1).$$

Wir überlassen es dem Leser/der Leserin zu überprüfen, dass dies in der Tat ein Codewort ist. (Das entsprechende Polynom ist $2x$.)

3.3 Das Fehlerauswertungspolynom

In diesem Abschnitt benutzen wir die gleichen Bezeichnungen wie im Abschnitt 3.2. Insbesondere ist der Auswertungsvektor $(1, \beta, \beta^2, \ldots, \beta^{n-1})$, wobei $\beta \in \mathbb{F}_q$

ein Element der Ordnung n ist. Wir schreiben $I = \{0 \leq i \leq n-1 \mid e_i \neq 0\}$ für die Menge der Fehlerstellen.

In Beispiel 3.2.2 haben wir schon eine Methode zur Berechnung der Fehlerwerte kennen gelernt. In diesem Abschnitt besprechen wir eine alternative Methode. Diese benutzt das Fehlerauswertungspolynom R.

Satz 3.3.1 (Forney-Formel) *Sei Λ das Fehlerstellenpolynom und R das Fehlerauswertungspolynom. Dann gilt*

$$e_i = -\frac{R(\beta^i)}{(\beta^i)^{2t+1}\Lambda'(\beta^i)}.$$

Beweis: Wir wissen, dass $\Lambda(x) = \prod_{i\in I}(x-\beta^i)$ ein normiertes Polynom vom Grad τ und R ein Polynom mit $\mathrm{Grad}(R) \leq \tau - 1$ ist. Da die Nullstellen von Λ paarweise verschieden sind, gilt für die Partialbruchzerlegung

$$\frac{R}{\Lambda} = \sum_{i\in I} \frac{R(\beta^i)}{\Lambda'(\beta^i)} \frac{1}{x-\beta^i},$$

wobei Λ' die formale Ableitung von Λ ist.

Um den Satz zu beweisen, berechnen wir das Residuum $R(\beta^i)/\Lambda'(\beta^i)$ von β^i in der Partialbruchzerlegung von R/Λ mit Hilfe der Schlüsselgleichung auf eine andere Weise.

Satz 3.2.6 impliziert die Existenz eines Polynoms T mit $\Lambda \cdot S = R + x^{2t}T$. Also gilt

$$\frac{R}{\Lambda} = S - \frac{x^{2t}T}{\Lambda}. \tag{3.7}$$

Das nachfolgende Lemma 3.3.2 zeigt die Existenz eines Polynoms U mit

$$S = \frac{C}{\Lambda} + \frac{x^{2t}U}{\Lambda},$$

wobei

$$\frac{C}{\Lambda} = -\left(\sum_{i\in I} e_i(\beta^i)^{2t+1}\frac{1}{x-\beta^i}\right). \tag{3.8}$$

Einsetzen in (3.7) liefert also

$$R \equiv C \pmod{x^{2t}}.$$

Da R und C Polynome vom Grad kleiner gleich $t-1$ sind, folgt, dass $R = C$. Damit ist der Satz gezeigt. □

Lemma 3.3.2 *Das Syndrompolynom erfüllt*

$$S = \sum_{i\in I} e_i\beta^i \frac{x^{2t} - (\beta^i)^{2t}}{x-\beta^i} = -\left(\sum_{i\in I} e_i(\beta^i)^{2t+1}\frac{1}{x-\beta^i}\right) + \frac{x^{2t}U}{\Lambda}$$

für ein Polynom U.

Beweis: Die Definition 1.4.2 des Syndrompolynoms impliziert

$$\begin{aligned} S(x) &= \sum_{j=0}^{2t-1} S_{2t-j} x^j = \sum_{j=0}^{2t-1} \left(\sum_{i \in I} e_i (\beta^i)^{2t-j} \right) x^j \\ &= \sum_{i \in I} e_i \left(\sum_{j=0}^{2t-1} (\beta^i)^{2t-j} x^j \right) = \sum_{i \in I} e_i (\beta^i)^{2t} \sum_{j=0}^{2t} \left(\frac{x}{\beta} \right)^j \\ &= \sum_{i \in I} e_i \beta^i \frac{x^{2t} - (\beta^i)^{2t}}{x - \beta^i}. \end{aligned}$$

Dies zeigt die erste Geichheit des Lemmas. Die zweite Gleichheit folgt direkt aus der ersten. □

Korollar 3.3.3 *Sei Λ das Fehlerstellenpolynom und R das Fehlerauswertungspolynom. Dann ist* $\mathrm{ggT}(R, \Lambda) = 1$.

Beweis: Nach Definition ist $\Lambda(x) = \prod_{i \in I}(x - \beta^i)$, wobei $I = \{i \mid e_i \neq 0\}$. Aus Satz 3.3.1 folgt direkt, dass $R(\beta^i) \neq 0$ für $i \in I$. □

Beispiel 3.3.4 Wir benutzen Satz 3.3.1, um die Fehlerwerte aus Beispiel 3.2.7.(b) nochmals zu berechnen. Wir haben schon berechnet, dass

$$\Lambda(x) = x - 2, \qquad R(x) = 1.$$

Der Fehlerwert ist also

$$e_1 = \frac{R(2)}{2^5 \Lambda'(2)} = \frac{1}{2 \cdot 1} = 3.$$

Wir finden das gleiche Ergebnis wie in Beispiel 3.2.7.(b).

3.4 Der euklidische Algorithmus

Im Beispiel 3.2.7.(b) haben wir das Fehlerstellenpolynom aus der Schlüsselgleichung berechnet, indem wir ein Gleichungssystem gelöss t haben. Im nächsten Abschnitt besprechen wir eine alternative, effizientere Methode basierend auf dem euklidischen Algorithmus. In diesem Abschnitt wiederholen wir den euklidischen Algorithmus und beweisen einige zusätzliche Eigenschaften.

Sei $\mathbb{F} = \mathbb{F}_q$ ein endlicher Körper. Das folgende Lemma fasst die Eigenschaften des ggTs zweier Polynome zusammen. Für einem Beweis verweisen wir auf [1, Kor. 3.3.6].

Lemma 3.4.1 *Seien $f, g \in \mathbb{F}[x]$ nicht beide Null und sei $d := \mathrm{ggT}(f, g)$.*

(a) Es existieren Polynome $a, b \in \mathbb{F}[x]$ mit

$$d(x) = a(x)f(x) + b(x)g(x).$$

(b) Jedes Polynom, das sich als $a(x)f(x)+b(x)g(x)$ darstellen lässt, ist durch $d(x)$ teilbar.

Die Polynome $d(x), a(x)$ und $b(x)$ aus Lemma 3.4.1 kann man mit Hilfe des erweiterten euklidischen Algorithmus berechnen. Einfachheitshalber nehmen wir an, dass $0 < \text{Grad}(g) \leq \text{Grad}(f)$. Wir definieren

$$\begin{aligned} \rho_{-1} &= f, & \rho_0 &= g, \\ a_{-1} &= 1, & a_0 &= 0 \\ b_{-1} &= 0, & b_0 &= 1. \end{aligned} \tag{3.9}$$

Für $i \geq 1$ definieren wir rekursiv Polynome ρ_i, q_i, a_i, b_i durch

$$\begin{aligned} \rho_i &= \rho_{i-2} - q_i \cdot \rho_{i-1}, \\ a_i(x) &= a_{i-2} - q_i \cdot a_{i-1}, \\ b_i(x) &= b_{i-2} - q_i \cdot b_{i-1}, \end{aligned} \tag{3.10}$$

wobei q_i durch die Bedingung $\text{Grad}(\rho_i) < \text{Grad}(\rho_{i-1})$ bestimmt wird. Anders gesagt: q_i ist der Quotient der Division von ρ_i durch ρ_{i-1}. Das Verfahren terminiert, wenn $\rho_m = 0$. In diesem Fall ist $\text{ggT}(f, g) = \rho_{m-1}(x)$.

Man zeigt leicht, dass für alle $-1 \leq i < m$ gilt

$$\rho_i(x) = a_i(x)f(x) + b_i(x)g(x). \tag{3.11}$$

Für $i = m - 1$ erhalten wir die Polynome $a = a_{m-1}, b = b_{m-1}$ aus Lemma 3.4.1.(a).

Lemma 3.4.2 *Wir benutzen die obigen Bezeichnugen.*

(a) Für $0 \leq i \leq m - 1$ gilt

$$\text{Grad}(b_i) + \text{Grad}(\rho_{i-1}) = \text{Grad}(f).$$

(b) Die Polynome a_i und b_i sind teilerfremd für $1 \leq i \leq m - 1$.

Beweis: Wir betrachten die Grade der Polynome in der ersten Gleichung aus (3.10). Wir wissen, dass $\text{Grad}(\rho_i) < \text{Grad}(\rho_{i-1}) < \text{Grad}(\rho_{i-2})$. Dies impliziert, dass

$$\text{Grad}(\rho_{i-2}) = \text{Grad}(q_i \cdot \rho_{i-1}) = \text{Grad}(q_i) + \text{Grad}(\rho_{i-1}) \tag{3.12}$$

und $\text{Grad}(q_i) > 0$ für $1 \leq i \leq m - 1$.

Aus der Definition der b_i (3.10) folgt mit Induktion, dass $\text{Grad}(b_{i-1}) > \text{Grad}(b_{i-2})$ und deshalb

$$\text{Grad}(b_i) = \text{Grad}(b_{i-1}) + \text{Grad}(q_i). \tag{3.13}$$

Wir zeigen Aussage (a) mit vollständiger Induktion. Für $i = 0$ gilt $b_0 = 1$ und $\rho_{-1} = f$, also stimmt die Aussage.

Wir nehmen an, dass die Aussage für $i-1$ gilt. Dann ist

$$\begin{aligned}\mathrm{Grad}(\rho_{i-1}) &\overset{(3.12)}{=} \mathrm{Grad}(\rho_{i-2}) - \mathrm{Grad}(q_i)\\ &\overset{\text{I.H.}}{=} \mathrm{Grad}(f) - \mathrm{Grad}(q_i) - \mathrm{Grad}(b_{i-1})\\ &\overset{(3.13)}{=} \mathrm{Grad}(f) - \mathrm{Grad}(b_i).\end{aligned}$$

Hiermit ist Aussage (a) gezeigt.

(b) Wir schreiben die Rekurrenz für die Polynome a_i und b_i aus (3.10) in Matrixform als

$$M_i = M_{i-1}Q_i,$$

wobei

$$M_i := \begin{pmatrix} a_i & a_{i-1} \\ b_i & b_{i-1}\end{pmatrix}, \qquad Q_i := \begin{pmatrix} -q_i & 1 \\ 1 & 0\end{pmatrix}.$$

Wir finden

$$\det(M_0) = \begin{vmatrix} 0 & 1 \\ 1 & 0\end{vmatrix} = -1 \qquad \det(Q_i) = -1.$$

Mit Induktion folgt, dass

$$\pm 1 = \det(M_i) = a_i b_{i-1} - a_{i-1}b_i.$$

Aussage (b) folgt hieraus. □

3.5 Decodieren mit Hilfe des euklidischen Algorithmus

Der folgende Algorithmus berechnet das Fehlerstellenpolynom mit Hilfe des euklidischen Algorithmus.

Algorithmus 3.5.1 Input: Ein Wort r mit $\tau \le t$ Fehlerstellen. Output: Ein Codewort c mit $d(c,r) \le t$.

(I) (*Vorbereitung*) Wir haben ein (fehlerhaftes) Wort r empfangen. Wir nehmen an, dass die Anzahl $\tau = |I|$ der Fehlerstellen $1 \le \tau \le t = \lfloor (n-k)/2 \rfloor$ erfüllt. Wir berechnen das Syndrompolynom S (Definition 3.2.4).

(II) (*Berechnung des Fehlerstellen- und Fehlerauswertungspolynoms*) Wir wenden den euklidischen Algorithmus auf $\rho_{-1}(x) := x^{2t}$ und $\rho_0 := S(x)$ an. Wir schreiben $\rho_j(x)$ für die Reste im euklidischen Algorithmus und b_j für die Polynome mit

$$\rho_j(x) \equiv b_j(x)S(x) \pmod{x^{2t}}. \tag{3.14}$$

Wir berechnen die Polynome ρ_j, b_j für $j = 1, \ldots, m$, wobei m minimal mit $\mathrm{Grad}(\rho_m) < t$ ist. Sei c der führende Koeffizient von b_m. Dann ist $\Lambda(x) := b_m(x)/c$ das Fehlerstellenpolynom und $R(x) := \rho_m(x)/c$ das Fehlerauswertungspolynom.

(III) (*Berechnung der Fehlerstellen*) Wir berechnen die Nullstellen von Λ durch Auswerten von $\Lambda(\beta^i)$. Die Nullstellen entsprechen den Fehlerstellen I.

(IV) (*Berechnung der Fehlerwerte*) Wir berechnen die Fehlerwerte (e_i) mit Hilfe der Formel aus Satz 3.3.1.

(V) Das gesuchte Codewort ist $c = r - e$.

Das folgende Theorem zeigt, dass Algorithmus 3.5.1 funktioniert. Es reicht zu zeigen, dass der Algorithmus das Fehlerstellenpolynom berechnet. Satz 3.3.1 zeigt, dass die von uns berechneten e_i dann auch die Fehlerwerte sind.

Theorem 3.5.2 *Seien (Λ, R) wie in Algorithmus 3.5.1. Dann ist Λ das Fehlerstellenpolynom und R das Fehlerauswertungspolynom.*

Beweis: Gleichung (3.14) zeigt, dass das Tupel (b_m, ρ_m) die Schlüsselgleichung (3.5) erfüllt. Die Wahl von m impliziert, dass $\mathrm{Grad}(\rho_m) < t$ und $\mathrm{Grad}(\rho_{m-1}) \geq t$ ist. Lemma 3.4.2.(a) zeigt, dass

$$\mathrm{Grad}(b_m) = \mathrm{Grad}(x^{2t}) - \mathrm{Grad}(\rho_{m-1}) \leq 2t - t = t.$$

Sei Λ das Fehlerstellenpolynom und R das Fehlerauswertungspolynom. Dann erfüllen (Λ, R) und (b_m, ρ_m) beide die Schlüsselgleichung (3.5), d.h.

$$\Lambda S \equiv R \pmod{x^{2t}}, \qquad b_m S \equiv \rho_m \pmod{x^{2t}}.$$

Wir schließen, dass

$$\rho_m \Lambda \equiv b_m \Lambda S \equiv b_m R \pmod{x^{2t}}. \tag{3.15}$$

Die Polynome ρ_m und R (bzw. b_m und Λ) haben Grad kleiner gleich $t-1$ (bzw. t). Es folgt, dass $\mathrm{Grad}(\rho_m \Lambda) < 2t$ und $\mathrm{Grad}(b_m R) < 2t$. Also folgt aus (3.15), dass

$$\rho_m \Lambda = R b_m.$$

Korollar 3.3.3 zeigt, dass $\mathrm{ggT}(R, \Lambda) = 1$. Lemma 3.4.2.(b) impliziert, dass $\mathrm{ggT}(b_m, \rho_m) = 1$. Nach Division von b_m und ρ_m durch den führenden Koeffizienten von b_m folgt also, dass

$$\Lambda = b_m, \qquad R = \rho_m.$$

Damit ist alles gezeigt. □

Beispiel 3.5.3 (a) Wir betrachten den $(5, 3, 3)$-Code aus Beispiel 3.1.4. Dieser Code hat Minimaldistanz $d = 3$ und kann daher $t = 1$ Fehler korrigieren. Wir haben das Wort $r = (\alpha, \alpha^{13}, \alpha^{11}, \alpha^{14}, \alpha^7)$ empfangen. Als Polynom geschrieben gilt

$$r(x) = \alpha + \alpha^{13} x + \alpha^{11} x^2 + \alpha^{14} x^3 + \alpha^7 x^4.$$

Also gilt $S_1 = r(\beta) = r(\alpha^3) = \alpha$ und $S_2 = r(\beta^2) = S(\alpha^6) = \alpha$ und das Syndrompolynom ist $S(x) = \alpha + \alpha x$.

Wir wenden den erweiterten euklidischen Algorithmus auf $\rho_{-1}(x) = x^{2t} = x^2$ und $\rho_0(x) = S(x)$ an und erhalten

i	ρ_i	q_i	b_i
-1	x^2	$-$	0
0	$\alpha + \alpha x$	$-$	1
1	1	$\alpha^{14}(x+1)$	$\alpha^{14}(x+1)$.

Der Algorithmus terminiert hier da $\text{Grad}(\rho_1) = 0 < t = 1$. Wir finden $\Lambda = x + 1 = x - \beta^0$ und $R = \alpha$. Die einzige Fehlerstelle ist also $i = 0$.

Als Nächstes berechnen wir der Fehlerwert

$$e_0 = -\frac{R(1)}{1^{2t+1}\Lambda'(1)} = \alpha.$$

Das gesuchte Codewort ist $c = r - e = (0, \alpha^{13}, \alpha^{11}, \alpha^{14}, \alpha^7)$.

Alternativ können wir auch die Methode aus Beispiel 3.2.7.(b) anwenden: Auflösen der Gleichung $\alpha = S_1 = \sum_{i \in I} e_i \beta^i = e_0$ liefert ebenfalls das gewünschte Ergebnis.

(b) Sei $\alpha \in \mathbb{F}_{16}$ ein Element mit $\alpha^4 + \alpha + 1$. Wir betrachten den $(15, 9)$-RS-Code mit Auswertungsvektor $(1, \alpha, \alpha^2, \ldots, \alpha^{14})$. Die Minimaldistanz ist $d_{\min} = n + 1 - k = 7$, also kann dieser Code $t = 3$ Fehler korrigieren.

Wir haben das Wort

$$r(x) = \alpha^7 x^8 + \alpha^{12} x^6 + \alpha^3 x^4 + \alpha^{14} x^3 + \alpha^{14} x^2$$

empfangen. Das Syndrompolynom ist also $S(x) = \alpha^9 + \alpha^{13} x + x^3 + \alpha^{12} x^4 + \alpha^2 x^5$.

Der erweiterte euklidische Algorithmus liefert:

i	ρ_i	q_i	b_i
-1	x^6	$-$	0
0	S	$-$	1
1	$\alpha^7 x^4 + \alpha^8 x^3 + \alpha^{11} x^2 + \alpha^{10} x + \alpha^2$	$\alpha^{13} x + \alpha^8$	$\alpha^{13} x + \alpha^8$
2	$\alpha^4 x^3 + \alpha^{12} x^2 + \alpha^{12} x + \alpha^6$	$\alpha^{10} x + \alpha^3$	$\alpha^8 x^2 + \alpha^9 x + \alpha^{12}$
3	$\alpha^3 x^2 + \alpha^9 x + \alpha^{10}$	$\alpha^3 x + \alpha^{13}$	$\alpha^{11} x^3 + \alpha^4 x^2 + \alpha^{10}$.

Das Fehlerstellenpolynom ist

$$\Lambda(x) = \frac{b_3}{\alpha^{11}} = (x - \alpha^{10})(x - \alpha^{13})(x - \alpha^{12}).$$

Für die Fehlerwerte finden wir $e_{10} = \alpha^7, \quad e_{12} = \alpha^5, \quad e_{13} = \alpha^8$. Das gesendete Codewort ist daher

$$c(x) = r(x) - e(x) = \alpha^8 x^{13} + \alpha^7 x^{10} + \alpha^5 x^{12} + \alpha^7 x^8 + \alpha^{12} x^6 + \alpha^3 x^4 + \alpha^{14} x^3 + \alpha^{14} x^2.$$

Mit Hilfe der Prüfmatrix kann man nachrechnen, dass c in der Tat ein Codewort ist. Alternativ kann man mit Hilfe von Polynominterpolation überprüfen, dass $c_i = f(\alpha^i)$, wobei

$$f(x) = x^7 + \alpha^4 x^6 + \alpha^{10} x^5 + \alpha^9 x^4 + \alpha^3 x^3 + \alpha^6 x^2 + \alpha^{12} x + \alpha^2.$$

4 Zyklische Codes

Fast alle Codes, die wir bisher betrachtet haben, sind sogenannte zyklische Codes. Beispiele sind die zyklischen RS-Codes (Definition 3.1.3) und die $(n, 1)$-Wiederholungscodes. Auch der berühmte Golay-Code ist ein zyklischer Code. Dieser Code wurde von der NASA bei den Voyager-Missionen benutzt, um Bilder von Jupiter und Saturn zur Erde zu schicken.

4.1 Eine algebraische Beschreibung zyklischer Codes

Definition 4.1.1 Ein linearer Code $\mathcal{C} \subset \mathbb{F}_q^n$ heißt *zyklisch*, wenn jede zyklische Verschiebung eines Codeworts wieder ein Codewort ist, d.h.

$$c = (c_0, \ldots, c_{n-2}, c_{n-1}) \in \mathcal{C} \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}.$$

Beispiel 4.1.2 (a) Sei $\mathcal{C} \subset \mathbb{F}_q^n$ der $(n, 1)$-Wiederholungscode (Beispiel 1.2.5). Dies ist offensichtlich ein zyklischer Code, da die zyklische Verschiebung die Codewörter $c = (c_0, c_0, \ldots, c_0)$ nicht verändert.

(b) Wir betrachten den $(7, 3)$-Code $\mathcal{C} \subset \mathbb{F}_2^7$ mit Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \in M_{3,7}(\mathbb{F}_2).$$

Wir schreiben v_1, v_2, v_3 für die Zeilen von G. Dann besteht $\mathcal{C}$ aus den Codewörtern $0, v_1, v_2, v_3$ und

$$\begin{aligned} v_1 + v_2 &= \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \\ v_1 + v_3 &= \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}, \\ v_2 + v_3 &= \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}, \\ v_1 + v_2 + v_3 &= \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}. \end{aligned}$$

Zyklische Verschiebung wie in Definition 4.1.1 fixiert das Wort $0 = (0, \ldots, 0)$ und vertauscht die übrigen 7 Wörter wie folgt:

$$v_1 \mapsto v_1 + v_2 \mapsto v_1 + v_2 + v_3 \mapsto v_2 + v_3 \mapsto v_1 + v_3 \mapsto v_2 \mapsto v_3 \mapsto v_1.$$

Dieser Code ist also zyklisch.

(c) Sei $\mathcal{C} = RS^{n,k}(\beta) \subset \mathbb{F}_q^n$ ein zyklischer RS-Code. Sei $f \in P_k$ ein Polynom von Grad kleiner gleich $k-1$ und $c = (f(1), f(\beta), \ldots, f(\beta^{n-1})) \in \mathcal{C}$ das entsprechende Codewort. Die zyklische Verschiebung von c ist

$$\tilde{c} := (f(\beta^{n-1}), f(1), f(\beta), \ldots, f(\beta^{n-2})).$$

Das Polynom $\tilde{f}(x) := f(\beta^{n-1}x)$ besitzt den gleichen Grad wie f und ist deshalb ebenfalls in P_k. Es gilt $\tilde{f}(\beta^i) = f(\beta^{i-1})$, da $\beta^n = 1$. Also ist

$$\tilde{c} = (f(\beta^{n-1}), f(1), f(\beta), \ldots, f(\beta^{n-2})) = (\tilde{f}(1), \tilde{f}(\beta), \ldots \tilde{f}(\beta^{n-1})) \in \mathcal{C}.$$

Ziel dieses Abschnitts ist es, eine algebraische Beschreibung von zyklischen Codes zu geben. Für diese Beschreibung brauchen wir folgenden Ring.

Definition 4.1.3 Wir definieren

$$\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - 1).$$

Die Elemente von $\mathcal{R}_n$ sind Nebenklassen $f + (x^n - 1)$. Jedes Polynom $f \in \mathbb{F}_q[x]$ ist kongruent modulo $x^n - 1$ zu einem eindeutig bestimmten Polynom vom Grad kleiner gleich $n-1$. Die Elemente von $\mathcal{R}_n$ können daher mit den Polynomen vom Grad kleiner gleich $n-1$ identifiziert werden. Wir sehen, dass $\mathcal{R}_n$ ein n-dimensionaler $\mathbb{F}_q$-Vektorraum ist.

Ist also $\mathcal{C} \subset \mathbb{F}_q^n$ ein Code, dann können wir $\mathcal{C}$ auch als Untervektorraum von $\mathcal{R}_n$ auffassen. Ein Codewort $c = (c_0, c_1, \ldots, c_{n-1})$ fassen wir dabei als Codepolynom

$$c(x) := c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \in \mathcal{R}_n$$

auf. Wir werden nicht zwischen Codewörtern und Codepolynomen unterscheiden. Der *Grad* eines Polynoms $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \in \mathcal{R}_n$ ist die größte Zahl $0 \neq m \leq n-1$ mit $c_m \neq 0$.

Zusätzlich zu der Vektorraumstruktur besitzt der Ring $\mathcal{R}_n$ eine Multiplikation. Um die Multiplikation in $\mathcal{R}_n$ zu beschreiben, reicht es die Multiplikation eines Polynoms mit x zu beschreiben. In $\mathcal{R}_n$ gilt die Relation $x^n = 1$, also finden wir:

$$\begin{aligned} x\cdot(c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}) &= c_0 x + c_1 x^2 + \cdots + c_{n-1}x^n \\ &\equiv c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1} \pmod{x^n - 1}. \end{aligned} \tag{4.1}$$

Dies entspricht also der zyklischen Verschiebung der Koeffizienten.

Achtung: Der Ring $\mathcal{R}_n$ ist kein Körper. Beispielsweise gilt

$$(x-1)(1 + x + \cdots + x^{n-1}) = x^n - 1 = 0 \in \mathcal{R}_n.$$

Das Element $x-1$ ist ein nicht-trivialer Nullteiler in $\mathcal{R}_n$. Insbesondere ist $x-1$ keine Einheit.

Der folgende Satz beschreibt zyklische Codes der Länge n als Ideale in $\mathcal{R}_n$.

Satz 4.1.4 *Ein zyklischer Code $\mathcal{C}$ der Länge n ist ein Ideal in $\mathcal{R}_n$, d.h.*

(a) *Für alle* $b(x), c(x) \in \mathcal{C}$ *ist* $b(x) + c(x) \in \mathcal{C}$.

(b) *Für alle* $c(x) \in \mathcal{C}$ *und* $f(x) \in \mathcal{R}_n$ *ist* $f(x)c(x) \in \mathcal{C}$.

Beweis: Der Code $\mathcal{C}$ ist ein Untervektorraum von $\mathcal{R}_n$, hieraus folgt (a) und (b) für konstante Polynome f. Um dem Satz zu beweisen, reicht es (b) für $f = x$ zu beweisen. Sei $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \in \mathcal{C}$. Dann sagt (4.1), dass

$$\tilde{c}(x) := x \cdot c(x) = c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1} \in \mathcal{R}_n.$$

Der Code $\mathcal{C}$ ist zyklisch, also ist $\tilde{c}(x) \in \mathcal{C}$. □

Satz 4.1.4 zeigt insbesondere , dass $\mathcal{C}$ abgeschlossen gegenüber die Multiplikation von Codepolynome ist. Diese zusätzliche Struktur werden wir im rest des Abschnittes benutzen, um eine alternative Beschreibung von zyklischen Codes als Ideale zu geben. Zuerst wiederholen wir einige Fakten über Ideale in kommutativen Ringen R aus [1, Abschnitte 3.2 und 3.3]. Uns interessieren nur die Ringe $\mathcal{R}_n$ und $\mathbb{F}_q[x]$ betrachten.

Ein Ideal $I < R$ heißt *Hauptideal*, wenn I von einem Element g erzeugt wird. Dies bedeutet, dass

$$I = \langle g \rangle = \{fg \mid f \in R\}$$

genau aus den Vielfachen von g besteht. Ist I von g erzeugt, dann heißt g ein *Erzeuger* von I.

Der Ring $\mathbb{F}_q[x]$ ist ein *Hauptidealring*, d.h. jedes Ideal $I < \mathbb{F}_q[x]$ ist ein Hauptideal ([1, Theorem 3.3.4]). Sei $I \subsetneq \mathbb{F}_q[x]$ ein Ideal mit $I \neq (0)$. Dann ist das normierte Polynom $g \in I \setminus \{0\}$ kleinsten Grades ein Erzeuger von I.

Theorem 4.1.5 *Sei* $\mathcal{C} < \mathcal{R}_n$ *ein zyklischer Code der Länge* n.

(a) *Das Ideal* $\mathcal{C}$ *ist ein Hauptideal.*

(b) *Sei* $g \in \mathcal{C} \setminus \{0\}$ *das normierte Polynom kleinsten Grades. Dann ist* g *ein Erzeuger von* $\mathcal{C}$ *und es gilt* $g \mid (x^n - 1) \in \mathbb{F}_q[x]$.

(c) *Ein Polynom* $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathcal{R}_n$ *ist genau dann in* $\mathcal{C}$*, wenn* $g(x) \mid c(x)$.

(d) *Die Dimension von* $\mathcal{C}$ *ist* $k = n - \mathrm{Grad}(g)$.

(e) *Ist umgekehrt* $g \mid (x^n - 1)$ *ein Teiler, dann ist* $\mathcal{C} = \langle g \rangle$ *ein zyklischer Code der Länge* k.

Beweis: Sei $\mathcal{C}$ ein zyklischer Code der Länge n, d.h. ein Ideal in $\mathcal{R}_n$. Wir betrachten die kanonische Abbildung

$$\pi : \mathbb{F}_q[x] \to \mathcal{R}_n, \qquad h \mapsto h \pmod{x^n - 1}.$$

Das Urbild $I := \pi^{-1}(\mathcal{C})$ ist ein Ideal von $\mathbb{F}_q[x]$. Da $\mathbb{F}_q[x]$ ein Hauptidealring ist, existiert ein Erzeuger g von I. Es folgt, dass $\pi(g)$ ein Erzeuger von $\mathcal{C} = \pi(I)$ ist. Dies zeigt (a). Es gilt $\pi(x^n - 1) = 0$, also ist $x^n - 1 \in I$. Dies impliziert,

dass $g \mid x^n - 1$. Insbesondere ist $\mathrm{Grad}(g) < n$ und wir können $\pi(g)$ mit g identifizieren. Hieraus folgt (b).

Wir schreiben $\mathrm{Grad}(g) = n - k$ und $g(x) = \sum_{i=0}^{n-k} g_i x^i$ mit $g_{n-k} = 1$. Die Elemente des Ideals $\langle g \rangle < \mathcal{R}_n$ sind die Vielfachen $c(x) = f(x)g(x)$ von g. Hieraus folgt (c). Die Elemente c von $\mathcal{R}_n$ können wir als Polynome von Grad kleiner gleich $n-1$ darstellen. Ist $c(x) = f(x)g(x) \in \mathcal{C}$, dann ist also $\mathrm{Grad}(f) \leq n - 1 - (n-k) = k - 1$. Es folgt, dass $\dim_{\mathbb{F}_q} \mathcal{C} \leq k$.

Die Polynome

$$\begin{aligned} g(x) &= g_0 + \cdots + g_{n-k}x^{n-k}, \\ xg(x) &= g_0 x + \cdots + g_{n-k}x^{n-k+1}, \\ &\vdots \\ x^{k-1}g(x) &= g_0 x^{k-1} + \cdots + g_{n-k}x^{n-1} \end{aligned}$$

sind $\mathbb{F}_q$-linear unabhängig als Elemente von $\mathcal{R}_n$. Also ist die Dimension von $\mathcal{C}$ mindestens k. Es folgt, dass $\dim_{\mathbb{F}_q}(\mathcal{C}) = k$ ist. Dies zeigt (d).

Ist $g \mid x^n - 1 \in \mathbb{F}_q[x]$, dann definiert $\langle g \rangle < \mathcal{R}_n$ ein Ideal, d.h. einen zyklischen Code. Dies zeigt (e). □

Definition 4.1.6 Sei $\mathcal{C}$ ein zyklischer Code der Länge n. Das normierte Polynom $g \in \mathcal{R}_n$ mit $\mathcal{C} = \langle g \rangle$ und $g \mid (x^n - 1)$ heißt *Erzeugerpolynom* von $\mathcal{C}$.

Im Beweis von Theorem 4.1.5.(d) haben wir gezeigt, dass $(x^i g(x))_{i=0,\ldots,k-1}$ eine Basis von $\mathcal{C}$ ist. Das folgende Korollar folgt daher unmittelbar aus Theorem 4.1.5.

Korollar 4.1.7 *Sei $\mathcal{C}$ ein zyklischer (n,k)-Code mit Erzeugerpolynom $g(x) = \sum_{i=0}^{n-k} g_i x^i$. Dann ist*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & & & \\ & g_0 & g_1 & \cdots & g_{n-k} & & \\ & & \ddots & \ddots & & \ddots & \\ & & & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix} = \begin{pmatrix} g(x) & & & \\ & xg(x) & & \\ & & \ddots & \\ & & & x^{k-1}g(x) \end{pmatrix}$$

eine Erzeugermatrix von $\mathcal{C}$.

Beispiel 4.1.8 (a) Sei $\mathcal{C}$ der $(n,1)$-Wiederholungscode mit Alphabet $\mathbb{F}_q$. Das Erzeugerpolynom ist

$$g(x) = 1 + x + \cdots + x^{n-1}.$$

(b) Wir betrachten alle zyklischen $(7,3)$-Codes über $\mathbb{F}_2$. Das Erzeugerpolynom g eines solchen Codes ist ein Teiler von $x^7 - 1$ vom Grad $n - k = 4$. Es gilt

$$x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1) \in \mathbb{F}_2[x].$$

Es gibt also zwei mögliche Erzeugerpolynome, nämlich

$$g_1(x) = (x+1)(x^3+x+1) = x^4+x^3+x^2+1, \qquad g_2(x) = x^4+x^2+x+1.$$

Sei $\mathcal{C}$ der zyklische $(7,3)$-Code aus Beispiel 4.1.2.(b). Das Erzeugerpolynom teilt alle Codepolynome, also insbesondere $v_1(x) = 1+x^3+x^5+x^6$. Dieses Polynom entspricht dem Codewort v_1. Wir finden $\mathrm{ggT}(v_1, g_1) = g_1$ und $\mathrm{ggT}(v_1, g_2) = (x+1)$. Das Erzeugerpolynom ist also g_1.

Eine andere Möglichkeit das Erzeugerpolynom zu berechnen folgt aus der Tatsache, dass das Erzeugerpolynom der größte gemeinsame Teiler der Basis $v_1(x), v_2(x), v_3(x)$ des Codes ist.

4.2 Das Prüfpolynom

Sei $\mathcal{C}$ ein zyklischer (n,k)-Code mit Erzeugerpolynom $g(x)$. Dann ist $g \mid (x^n-1)$ (Definition 4.1.6), also ist $h(x) = (x^n-1)/g(x)$ ebenfalls ein Teiler von x^n-1. Der Grad von g ist $n-k$, also ist $\mathrm{Grad}(h) = k$.

Definition 4.2.1 Sei $\mathcal{C}$ ein zyklischer Code der Länge n mit Erzeugerpolynom g. Das Polynom $h(x) := (x^n-1)/g(x)$ heißt *Prüfpolynom*.

Der folgende Satz erklärt den Grund für diese Terminologie.

Satz 4.2.2 *Sei $\mathcal{C}$ ein zyklischer Code mit Erzeugerpolynom g und Prüfpolynom $h(x) = h_0 + h_1 x + \cdots + h_k x^k$.*

(a) Sei $c(x) \in \mathcal{R}_n$. Dann gilt

$$c(x) \in \mathcal{C} \quad \Leftrightarrow \quad c(x)h(x) = 0 \in \mathcal{R}_n.$$

(b) Die Matrix

$$H = \begin{pmatrix} & & & h_k & \cdots & h_1 & h_0 \\ & & h_k & \cdots & h_1 & h_0 & \\ & \iddots & & \iddots & \iddots & & \\ h_k & \cdots & h_1 & h_0 & & & \end{pmatrix}$$

ist eine Prüfmatrix von $\mathcal{C}$

Beweis: Die Codepolynome in $\mathcal{C} = \langle g \rangle \subset \mathcal{R}_n$ sind genau die Polynome der Form $c(x) = f(x)g(x)$. Für diese Polynome gilt also

$$c(x)h(x) = f(x)g(x)h(x) = f(x)(x^n-1) = 0 \in \mathcal{R}_n.$$

Dies zeigt (a).

Sei nun $c(x) = \sum_{i=0}^{n-1} c_i x^i$ ein Codepolynom. Der Koeffizient von x^j in $c(x)h(x)$ ist

$$\sum_{i=0}^{n-1} c_i h_{j-i}.$$

Wir rechnen im Ring $\mathcal{R}_n$, also betrachten wir die Indizes modulo n. Für $j = 0, \ldots, n-k-1$ finden wir $n-k$ linear unabhängige Prüfgleichungen. Hieraus folgt (b). □

Das folgende Korollar ist eine Variante von Satz 1.6.2 für zyklische Codes.

Korollar 4.2.3 *Sei $\mathcal{C}$ ein zyklischer Code mit Prüfpolynom $h(x)$. Dann ist der duale Code auch zyklisch mit Erzeugerpolynom*

$$g^\perp(x) = x^k h\left(\frac{1}{x}\right).$$

Das Polynom $x^k h(1/x)$ heißt das zu h *reziproke Polynom*. Ist $h(x) = h_0 + h_1 x + \cdots + h_k x^k$, dann ist das reziproke Polynom $h_k + h_{k-1}x + \cdots + h_0 x^k$.

Beweis: Die Prüfmatrix des Codes ist eine Erzeugermatrix des dualen Codes. Wir betrachten die Prüfmatrix H aus Satz 4.2.2.(b). Nach Umordnen der Zeilen finden wir die Matrix

$$G^\perp = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & & & \\ & h_k & h_{k-1} & \cdots & h_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix}.$$

Aus Korollar 4.1.7 folgt, dass der duale Code zyklisch mit Erzeugerpolynom

$$g^\perp(x) = h_k + h_{k-1}x + \cdots + h_0 x^k = x^k h\left(\frac{1}{x}\right)$$

ist. □

Beispiel 4.2.4 (a) Sei $g(x) = x^4 + x^3 + x^2 + 1$ das Erzeugerpolynom des $(7,3)$-Codes aus Beispiel 4.1.2.(b) und Beispiel 4.1.8.(b). Das Prüfpolynom ist

$$h(x) = \frac{x^7 - 1}{g} = x^3 + x^2 + 1.$$

Also ist $g^\perp(x) = x^3 + x + 1$ das Erzeugerpolynom des dualen Codes $\mathcal{C}^\perp$.

In Beispiel 1.6.4.(a) haben wir gesehen, dass der duale Code $\mathcal{C}^\perp$ der $(7,4)$-Code aus Beispiel 1.2.8 ist. Dieser Code ist daher auch zyklisch. Man kann dies auch direkt nachrechnen.

(b) Sei $\mathcal{C}$ ein selbstdualer zyklischer Code. Dann ist $g(x) = g^\perp(x)$ das reziproke Polynom des Prüfpolynoms. Ein Beispiel ist der $(n = 2k, k)$-Code über $\mathbb{F}_2$ mit Erzeugerpolynom $g(x) = x^k + 1$. In diesem Fall gilt

$$x^{2k} - 1 = (x^k + 1)(x^k - 1) = (x^k + 1)^2 \in \mathbb{F}_2[x].$$

Also ist $h(x) = g(x)$ und $g^\perp(x) = x^k h(1/x) = g(x)$.

4.3 Die Minimaldistanz eines zyklischen Codes

In diesem Abschnitt beweisen wir eine untere Schranke für die Minimaldistanz eines zyklischen Codes (Theorem 4.3.2). Im ganzen Abschnitt nehmen wir an, dass die Länge n des zyklischen Codes teilerfremd zur Charakteristik p des Körpers ist.

Sei $\mathcal{C}$ ein zyklischer (n,k)-Code über $\mathbb{F}_q$ mit Erzeugerpolynom $g(x)$. Wir schreiben $q = p^s$. Die Schranke, die wir beweisen möchten, benutzt die Nullstellen von $g(x)$. Nach Definition ist g ein Teiler von $x^n - 1$. Wir betrachten daher zunächst die Nullstellen von $x^n - 1$.

Sei m minimal, sodass $n \mid (q^m - 1)$. Die Zahl m existiert, da wir angenommen haben, dass n teilerfremd zu p, also auch zu $q = p^s$, ist. Im Körper $\mathbb{F}_{q^m} = \mathbb{F}_{p^{sm}}$ existiert ein Element β der Ordnung n, da $\mathbb{F}_{q^m}^*$ eine zyklische Gruppe der Ordnung $q^m - 1$ ist (Satz 2.1.5). In $\mathbb{F}_{q^m}$ gilt daher

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \beta^i).$$

Im Körper $\mathbb{F}_{q^m}$ zerfällt g als Faktor von $x^n - 1$ also in Linearfaktoren.

Beispiel 4.3.1 Wir betrachten das Polynom $g(x) := x^3 + x + 1$. Dies ist das Erzeugerpolynom des dualen Codes aus Beispiel 4.2.4.(a). Der zyklische Code $\mathcal{C} = \langle g \rangle$ ist ein $(7,4)$-Code über $\mathbb{F}_2$.

Wir haben $n = 7$. Die kleinste Zahl m mit $7 \mid (2^m - 1)$ ist $m = 3$. Man zeigt leicht, dass $g(x) \in \mathbb{F}_2[x]$ irreduzibel ist. Also ist

$$\mathbb{F}_8 \simeq \mathbb{F}_2[x]/(x^3 + x + 1).$$

Sei $\alpha \in \mathbb{F}_8$ eine Nullstelle von g. Dann folgt aus Satz 2.3.1.(b), dass

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4).$$

Theorem 4.3.2 (BCH-Schranke) *Sei $\mathcal{C}$ ein zyklischer Code mit Erzeugerpolynom g und sei $\mathbb{F}$ ein Körper in dem g in Linearfaktoren zerfällt. Wir wählen ein Element $\alpha \in \mathbb{F}^*$ der Ordnung n. Existieren $a, \delta \geq 0$, sodass*

$$g(\alpha^a) = g(\alpha^{a+1}) = \cdots = g(\alpha^{a+\delta-2}) = 0$$

dann gilt $d_{\min}(\mathcal{C}) \geq \delta$.

Beispiel 4.3.3 Wir betrachten das Polynom $g(x) = x^3 + x + 1$ aus Beispiel 4.3.1. Jedes Element $\alpha \in \mathbb{F}_8^*$ mit $\alpha \neq 1$ besitzt Ordnung $8 - 1 = 7$, also insbesondere auch die von uns gewählte Nullstelle von g. Wir haben gesehen, dass $g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$. Theorem 4.3.2 impliziert also, dass die Minimaldistanz des Codes

$$d_{\min}(\mathcal{C}) \geq 3$$

erfüllt. Das Erzeugerpolynom $g(x)$ ist selbst ein Element des Codes und besitzt Gewicht 3. Es folgt, dass $d_{\min}(\mathcal{C}) = 3$.

Der Code $\mathcal{C}$ ist der gleiche, den wir in Beispiel 1.2.8 betrachtet haben. In Beispiel 1.3.4 haben wir die Minimaldistanz schon auf andere Weise bestimmt.

Wir beweisen nun Theorem 4.3.2.

Beweis des Theorems: Wir möchten das Theorem mit Hilfe von Satz 1.3.3 beweisen. Die Prüfmatrix, die wir in Satz 4.2.2.(b) bestimmt haben, ist hierfür nicht geeignet, da wir das Prüfpolynom h nicht explizit kennen. Wir bestimmen daher eine alternative Prüfmatrix H.

Wir benutzen die Bezeichnungen des Theorems und definieren

$$\tilde{H} = \begin{pmatrix} 1 = \alpha^0 & \alpha^a & \alpha^{2a} & \cdots & \alpha^{(n-1)a} \\ 1 & \alpha^{a+1} & \alpha^{2(a+1)} & \cdots & \alpha^{(n-1)(a+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{a+\delta-2} & \alpha^{2(a+\delta-2)} & \cdots & \alpha^{(n-1)(a+\delta-2)} \end{pmatrix} \in M_{\delta-1,n}(\mathbb{F}).$$

Die Matrix $\tilde{H}$ ist selbst keine Prüfmatrix. Wir werden zeigen, dass $\tilde{H}$ ein Minor einer Prüfmatrix ist, d.h. die Zeilen definieren linear unabhängige Prüfgleichungen des Codes $\mathcal{C}$. Wir können die Matrix $\tilde{H}$ daher um $n + 1 - k - \delta$ weitere Prüfgleichungen ergänzen um eine Prüfmatrix H' zu erhalten. (Dies folgt aus dem Basisergänzungssatz.) Offensichtlich reicht die Kenntnis der Matrix $\tilde{H}$ aus um Satz 1.3.3 anzuwenden: Die minimale Anzahl μ der linear abhängigen Spalten von $\tilde{H}$ ist kleiner gleich die der Prüfmatrix H'. Es gilt also $\mu \leq d_{\min}(\mathcal{C})$.

Diese Diskussion zeigt, dass das Theorem aus folgenden zwei Behauptungen folgt:

(a) Es gilt $\tilde{H}c^t = 0$ für alle Codewörter $c \in \mathcal{C}$,

(b) Jede Wahl von $\delta - 1$ Spalten von $\tilde{H}$ sind linear unabhängig.

Sei $c(x) \in \mathcal{C}$ ein Codepolynom. Dann existiert ein Polynom f mit $c(x) = f(x)g(x)$, also ist $c(\alpha^a) = c(\alpha^{a+1}) = \cdots = c(\alpha^{a+\delta-2}) = 0$. Daher gilt, dass

$$\tilde{H} \cdot c^t = \begin{pmatrix} c(\alpha^a) \\ \vdots \\ c(\alpha^{a+\delta-1}) \end{pmatrix} = 0. \tag{4.2}$$

Behauptung (a) folgt.

Für (b) wählen wir $(\delta - 1)$ beliebige Spalten $s_{i_1}, \ldots, s_{i_{\delta-1}}$ von $\tilde{H}$, wobei $0 \leq i_1 < \cdots < i_{\delta-1} \leq n - 1$ ist. Der entsprechende Minor von $\tilde{H}$ ist

$$\tilde{H}(i) = \begin{pmatrix} \alpha^{i_1 a} & \cdots & \alpha^{i_{\delta-1} a} \\ \vdots & & \vdots \\ \alpha^{i_1(a+\delta-1)} & \cdots & \alpha^{i_{\delta-1}(a+\delta-1)}. \end{pmatrix}$$

Diese Matrix ist eine Variante einer Vandermonde-Matrix. Die Zahlen α^{i_j} sind paarweise verschiedene Elemente von $\mathbb{F}^*$. Wie im Beweis von Satz 3.1.5 folgt, dass $\det(\tilde{H}(i)) \neq 0$. Dies zeigt Behauptung (b). Wir haben schon gesehen, dass das Theorem aus den Behauptungen (a) und (b) folgt, also ist das Theorem bewiesen. □

Wir können die Idee aus dem Beweis von Theorem 4.3.2 benutzen, um das Erzeugerpolynom eines zyklischen RS-Codes zu bestimmen.

Satz 4.3.4 *Sei $\mathcal{C} = RS^{n,k}(\beta)$ ein zyklischer RS-Code. Insbesondere ist $\beta \in \mathbb{F}_q^*$ ein Element der Ordnung n. Dann ist*

$$g(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{n-k})$$

ein Erzeugerpolynom von $\mathcal{C}$.

Beweis: Satz 3.1.5 sagt, dass

$$H = \begin{pmatrix} 1 & \beta & \cdots & \beta^{n-1} \\ 1 & \beta^2 & \cdots & (\beta^2)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \beta^{n-k} & \cdots & (\beta^{n-k})^{n-1} \end{pmatrix}$$

eine Prüfmatrix von $\mathcal{C}$ ist. Hieraus folgt, dass

$$Hc^t = \begin{pmatrix} c(\beta) \\ \vdots \\ c(\beta^{n-k}) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad \text{für alle } c \in \mathcal{C}.$$

Es folgt, dass $\beta, \beta^2, \ldots, \beta^{n-k}$ gemeinsame Nullstellen aller Codewörter, also auch vom Erzeugerpolynom g, sind. Das Erzeugerpolynom g besitzt Grad $n-k$ und die Aussage des Satzes folgt. □

Die folgende Aussage benutzt ebenfalls die Idee von Theorem 4.3.2.

Satz 4.3.5 *Sei $\mathcal{C}$ ein zyklischer Code mit Erzeugerpolynom g. Wir nehmen an, dass $\beta, \beta^2, \ldots, \beta^{2t}$ Nullstellen von g sind. Dann kann Algorithmus 3.5.1 benutzt werden um t Fehler zu korrigieren.*

Beweisskizze: Sei $r = c + e$ ein empfangenes Wort. Der Algorithmus benutzt nur, dass die Zahlen $S_i = r(\beta^i)$ für $i = 1, \ldots, 2t$ Syndrome sind. Dies ist äquivalent zur Tatsache, dass $c(\beta^i) = 0$ für alle Codepolynome c und alle $i = 1, \ldots, 2t$. Dies folgt aus der Tatsache, dass das Erzeugerpolynom alle Codepolynome teilt. □

Der Satz zeigt, dass zyklische Codes ebenfalls mit dem euklidischen Algorithmus decodiert werden können. Sei t die Anzahl der Fehler, die der Algorithmus korrigieren kann. Dann folgt aus Theorem 4.3.2, dass $2t+1 \leq d_{\min}(\mathcal{C})$. Für RS-Codes ist $t = \lfloor (d_{\min}(\mathcal{C})-1)/2 \rfloor$, was nach Lemma 1.1.6 bestmöglich ist. Im Allgemeinen ist es möglich, dass $t < \lfloor (d_{\min}(\mathcal{C})-1)/2 \rfloor$ ist.

4.4 BCH-Codes

In diesem Abschnitt beschreiben wir eine Methode um Codes mit vorgegebener Minimaldistanz δ zu konstruieren. Diese Codes heißen BCH-Codes nach ihren Erfindern Bode, Ray-Chaudhuri und Hocquenghem.

Wir wählen ein Element $\beta \in \mathbb{F}_{q^s}^*$ der Ordnung n. Insbesondere gilt $n \mid (q-1)$. Wie in Abschnitt 2.3 definieren wir

$$M^{(i)} = \min_{\mathbb{F}_q}(\beta^i).$$

Satz 2.3.1.(b) und Korollar 2.3.4 implizieren, dass

$$M^{(i)} = (x-\beta^i)(x-\beta^{qi})\cdots(x-\beta^{q^{m_i-1}i}) \in \mathbb{F}_q[x],$$

wobei m_i die kleinste positive Zahl mit $q^{m_i} i \equiv i \pmod{q^s-1}$ ist.

Übungsaufgabe 4.4.1 Zeigen Sie, dass m_i ebenfalls die kleinste positive Zahl ist, sodass

$$n_i := \operatorname{ord}(\beta^i) = \frac{n}{\operatorname{ggT}(i,n)} \mid q^{m_i} - 1.$$

Der Körper $\mathbb{F}_{q^{m_i}}$ ist also die kleinste Körpererweiterung von $\mathbb{F}_q$, die ein Element der Ordnung n_i enthält.

Das Element β besitzt Ordnung n, also sind die Polynome $M^{(i)}$ Teiler von $x^n - 1$. Diese Polynome definieren daher zyklische Codes der Länge n über $\mathbb{F}_q$. Als Motivation für die Definition des BCH-Codes, zeigen wir zuerst, dass die Hamming-Codes definiert in Abschnitt 1.5 zyklisch sind und bestimmen deren Erzeugerpolynome.

Beispiel 4.4.2 (Hamming-Codes als zyklische Codes) Ein m-Hamming-Code $\mathcal{C}_m$, wie definiert in Abschnitt 1.5, ist ein $(n = 2^m - 1, k = 2^m - m - 1, 3)$-Code. Als Prüfmatrix betrachten wir eine Matrix $H_m \in M_{n-k,n}(\mathbb{F}_2)$ deren Spalten die verschiedenen Vektoren in $\mathbb{F}_2^m \setminus \{0\}$ sind.

Wir betrachten den Körper $\mathbb{F}_{2^m}$ und wählen ein Element $\alpha \in \mathbb{F}_{2^m}$ der Ordnung $2^m - 1$. Dies ist ein primitives Element, also können wir jedes Element aus $\mathbb{F}_{2^m}$ als Vektor bezüglich der Basis $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ schreiben. Insbesondere können wir die Spalten der Prüfmatrix auch als Elemente in $\mathbb{F}_{2^m}$ auffassen. Wir wählen

$$H_m = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \end{pmatrix}. \tag{4.3}$$

Hierbei interpretieren wir die Zahl $\alpha^i \in \mathbb{F}_{2^m}$ als Vektor in $\mathbb{F}_2^m$.

Beispielsweise für $m = 3$ wählen wir α mit Minimalpolynom $\min_{\mathbb{F}_2}(\alpha) = x^3 + x + 1$. Für H_m finden wir

$$H_m = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Sei nun $c \in \mathcal{C}_m$ ein Codewort und $c(x)$ das entsprechende Codepolynom. Mit Hilfe von (4.3) können wir die Prüfgleichung $H_m c^t = 0$ auch als $c(\alpha) = 0$ schreiben. Also ist α eine Nullstelle aller Codepolynome. Ist der Code zyklisch, dann ist α also auch eine Nullstelle des Erzeugerpolynoms $g(x)$.

Das Polynom $M^{(1)} = \min_{\mathbb{F}_2}(\alpha)$ ist ein Polynom in $\mathbb{F}_2[x]$ vom Grad $m = n-k$ (Lemma 2.2.4). Ein Polynom $c(x) \in \mathbb{F}_2[x]$ besitzt genau dann eine Nullstelle in α, wenn $c(x)$ von $M^{(1)}$ geteilt wird. Hieraus folgt, dass $\mathcal{C}_m = \langle M^{(1)} \rangle$ und $\mathcal{C}_m$ ist zyklisch mit Erzeugerpolynom $M^{(1)}$. Für $m = 3$ entspricht dies Beispiel 4.3.3.

Satz 4.4.3 *Sei n teilerfremd zu q und sei s die kleinste positive Zahl, sodass $n \mid (q^s - 1)$. Wir wählen $\beta \in \mathbb{F}_{q^s}^*$ ein Element der Ordnung n.*

Für $1 \leq \delta \leq n+1$ definieren wir $\mathcal{C}_\delta$ als den zyklischen Code über $\mathbb{F}_q$ mit Erzeugerpolynom

$$g(x) := \mathrm{kgV}(M^{(1)}, M^{(2)}, \ldots, M^{(\delta-1)}). \tag{4.4}$$

Der Code $\mathcal{C}_\delta$ besitzt Minimaldistanz $d_{\min}(\mathcal{C}_\delta) \geq \delta$ und Dimension $k \geq n - s(\delta - 1)$.

Beweis: Die Schranke für δ impliziert, dass die Zahlen $1, 2, \ldots, \delta-1$ modulo n paarweise verschieden sind. Das Polynom g besitzt offensichtlich $\beta, \beta^2, \ldots, \beta^{\delta-1}$ als Nullstellen. Die Schranke für die Minimaldistanz folgt daher aus Theorem 4.3.2.

Das Polynom $M^{(i)}$ besitzt Grad $m_i \leq s$. Es folgt, dass

$$k = n - \mathrm{Grad}(g) \geq n - (\delta - 1)s.$$

□

Definition 4.4.4 Die Codes aus Satz 4.4.3 heißen *BCH-Codes mit designierter Minimaldistanz* δ und Länge n.

Beispiel 4.4.5 (a) Hamming-Codes sind BCH-Codes mit designierter Minimaldistanz $\delta = 2$. Die echte Minimaldistanz ist aber 3, siehe Bemerkung 4.4.6.

(b) Zyklische RS-Codes sind auch BCH-Codes. Das Erzeugerpolynom g eines zyklischen RS-Codes $RS^{n,k}(\beta)$ über $\mathbb{F}_q$ zerfällt über $\mathbb{F}_q$ in Linearfaktoren, also ist $s = 1$. Die Minimalpolynome $M^{(i)} = \min_{\mathbb{F}_q}(\beta^i)$ haben daher Grad 1.

(c) Wir wählen $n = 10$ und $q = 3$. Die kleinste positive Zahl s, sodass 10 ein Teiler von $(3^s - 1)$ ist, ist $s = 4$. Sei $\beta \in \mathbb{F}_{3^4}$ ein Element der Ordnung $n = 10$. Um das Minimalpolynom $\min_{\mathbb{F}_3}(\beta)$ zu finden, betrachten wir die Faktorisierung von $x^{10} - 1$ in $\mathbb{F}_3[x]$ und finden

$$x^{10} - 1 = (x-1)(x+1)(x^4 - x^3 + x^2 - x + 1)(x^4 + x^3 + x^2 + x + 1).$$

Ähnlich wie im Beispiel 2.2.3 überlegt man sich, dass die Nullstellen der jeweiligen Faktoren Ordnung $1, 2, 10$ und 5 haben. Hieraus folgt, dass $M^{(1)} = \min_{\mathbb{F}_3}(\beta) = x^4 - x^3 + x^2 - x + 1$.

Die Faktorisierung von $M^{(1)}$ über $\mathbb{F}_{3^4}$ erhalten wir aus Satz 2.3.1:

$$M^{(1)} = (x-\beta)(x-\beta^3)(x-\beta^9)(x-\beta^7).$$

Hierbei haben wir benutzt, dass $\mathrm{ord}(\beta) = 10$. Mit dem gleichen Verfahren finden wir

i	$M^{(i)}$	Nullstellen	Ordnung
1	$x^4 - x^3 + x^2 - x + 1$	$\beta, \beta^3, \beta^9, \beta^7$	10
2	$x^4 + x^3 + x^2 + x + 1$	$\beta^2, \beta^6, \beta^8, \beta^4$	5
5	$x + 1$	$\beta^5 = -1$	2
10	$x - 1$	$\beta^0 = 1$	1

Wir möchten einem BCH-Code mit designierter Minimaldistanz $\delta = 3$ konstruieren. Das Erzeugerpolynom soll also β und β^2 als Nullstellen haben. Wir definieren

$$g(x) = M^{(1)} \cdot M^{(2)} = x^8 + x^6 + x^4 + x^2 + 1.$$

Die Dimension des Codes ist $k = n - \mathrm{Grad}(g) = 10 - 8 = 2$.

Das Polynom besitzt die Nullstellen $\beta, \beta^2, \beta^3, \beta^4$, also ist

$$5 \leq d_{\min}(\mathcal{C}) \leq n + 1 - k = 10 + 1 - 2 = 9.$$

Wir bemerken, dass $g(x) \in \mathcal{C}$ ein Wort vom Gewicht 5 ist. Also ist die Minimaldistanz 5.

Bemerkung 4.4.6 Ist $q = 2$, dann bekommen wir eine bessere Schranke für die Dimension eines BCH-Codes. In diesem Fall sind die $\beta^{2^j i}$ ebenfalls Nullstellen von $M^{(i)} = \min_{\mathbb{F}_2}(\beta^i)$. Also ist $M^{(i)} = M^{(2i)} = M^{(4i)} = \cdots$ Der Hamming-Code $\mathcal{C}_m$ aus Beispiel 4.4.2 ist ein BCH-Code mit designierter Minimaldistanz $\delta = 2$. Da α^2 eine Nullstelle von $M^{(1)}$ ist, ist der Code ebenfalls ein BCH-Code mit designierten Minimaldistanz $\delta = 3$. Die echte Minimaldistanz ist in der Tat 3 (Abschnitt 1.5).

Korollar 4.4.7 *Sei $q = 2$ und $\delta = 2t + 1$ ungerade. Desweiteren seien n, β und s wie in Satz 4.4.3. Der BCH-Code $\mathcal{C}$ aus Satz 4.4.3 besitzt Dimension*

$$k \geq n - st.$$

Beweis: Der BCH-Code $\mathcal{C}$ bezitzt Erzeugerpolynom

$$g(x) = \mathrm{kgV}(M^{(1)}, M^{(2)}, \ldots, M^{(2t)}) = \mathrm{kgV}(M^{(1)}, M^{(3)}, \ldots, M^{(2t-1)}).$$

Die letzte Gleichheit folgt aus Bemerkung 4.4.6. Das Argument aus dem Beweis von Satz 4.4.3 liefert sofort die Schranke aus der Aussage des Korollars. □

Beispiel 4.4.8 Die folgende Tabelle beschreibt die BCH-Codes mit designiertem Minimaldistanz δ für $q = 2$ und $n = 15$. Als Element $\beta \in \mathbb{F}_{2^4}$ wählen wir wie üblich eine Nullstelle von $x^4 + x + 1$.

Die entsprechenden Polynome $M^{(i)}$ und deren Nullstellen haben wir in Beispiel 2.3.5 berechnet. Man sieht leicht, dass das Erzeugerpolynom g_δ zu $\delta = 2t+1 \leq 9$ das Produkt $M^{(1)}M^{(3)}\cdots M^{(2t-1)}$ ist. Für $\delta \geq 9$ ändert sich das Erzeugerpolynom nicht mehr.

δ	$g(x)$	k	$d_{\min}(C_\delta)$
1	1	15	1
3	x^4+x+1	11	3
5	$x^8+x^7+x^6+x^4+1$	7	5
7	$x^{10}+x^8+x^5+x^4+x^2+x+1$	5	7
9	$x^{14}+x^{13}+\cdots+x^2+x+1$	1	15.

Literatur

[1] I.I. Bouw, *Elemente der Algebra*, Vorlesungsskript, WS 2012/2013.

[2] I.I. Bouw, *Elementare Zahlentheorie*, Vorlesungsskript, Sommersemester 2010.